PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-275203
(43)Date of publication of application : 13.10.1998

(51)Int.Cl. G06K 17/00
G06T 7/00
G06K 19/10
G06K 19/06
H04L 9/32

(21)Application number : 09-227979
(22)Date of filing : 25.08.1997

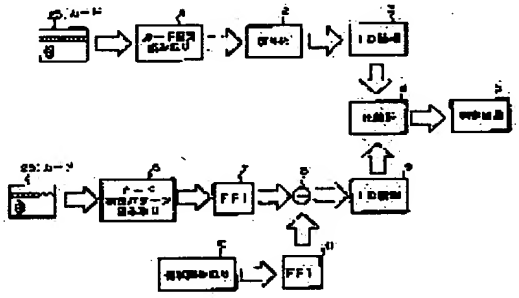
(71)Applicant : NEC CORP
(72)Inventor : TAKAI KAZUTO
FUJIWARA SHIRO

(30)Priority

Priority number	Priority date	Priority country
08317545	28.11.1996	JP
08357504	27.12.1996	JP
09 20602	03.02.1997	JP

(54) CARD TYPE RECORDING MEDIUM, METHOD AND DEVICE FOR ITS AUTHENTICATION, PREPARING SYSTEM, CIPHERING SYSTEM, ITS DECIPHERING DEVICE AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To improve security by providing information to input in a magnetic card for both of magnetic data and the pattern of the card to prevent a third party from easily duplicate the card and to discriminate when it is duplicated.
SOLUTION: Written fingerprint pattern written in the card 25 is read by a card image reader 6 and the image is Fourier-transformed at a high speed by FFT 7. On the other hand, the fingerprint pattern of the present owner himself is read by a fingerprint pattern reader 10 and the data is Fourier-transformed at a high speed by FFT 11. A subtracter 8 subtracts the output of FFT 11 from the output of FFT 7 to extract ID information specifying a user. In addition the magnetic data of the card 25 is read by a magnetic reader 1 and a decoding processor 2 deciphers the code to extract ID information 3. Then ID information 9 extracted from the card 25 and ID information 3 extracted from magnetic data are compared by a comparator 4 and a judging circuit 5 judges illegally duplicated information from the result.



LEGAL STATUS

[Date of request for examination]	25.08.1997
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3075221
[Date of registration]	09.06.2000
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of	

rejection]
[Date of extinction of right]

* NOTICES *

CLAIMS

[Claim(s)]
[Claim 1] In the card type record medium containing the picture image field where the data area on which the data containing an owner's ID information were recorded, and image data are recorded in the aforementioned picture image field Transform processing to the data of a frequency domain is performed to the 1st image data which specifies the owner itself. The card type record medium characterized by recording the 2nd image data generated by adding the aforementioned ID information to the data of the frequency domain after this conversion, and carrying out the inverse transformation of this added data to a picture signal.
[Claim 2] ID information on the aforementioned data area is a card type record medium according to claim 1 characterized by what is enciphered and recorded.
[Claim 3] The 1st aforementioned image data is a card type record medium according to claim 1 or 2 characterized by being an owner's fingerprint picture image or photograph-of-his-face picture image.
[Claim 4] Transform processing to the data of the aforementioned frequency domain is the claim 1 characterized by being Fourier transformation, or a card type record medium given in 2 and 3.
[Claim 5] Transform processing to the data of the aforementioned frequency domain is the claim 1 characterized by being the discrete cosine conversion given to each of the block which divides the 1st aforementioned image data into plurality, and is acquired, or a card type record medium given in 2 and 3.
[Claim 6] It is a card type record medium containing the picture image field where the data area on which the data containing an owner's ID information were recorded, and image data are recorded. in the aforementioned picture image field Transform processing to the data of a frequency domain is performed to the 1st image data which specifies the owner itself. It is the card type record-medium authentication technique that the 2nd image data generated by adding the aforementioned ID information to the data of the frequency domain after this conversion, and carrying out the inverse transformation of this added data to a picture signal is recorded. The 1st step which reads the data of the aforementioned picture image field while the aforementioned ID information is restored from the aforementioned card type record medium, The 2nd step which performs transform processing to the data of a frequency domain to the data of the aforementioned picture image field, and generates the 1st resolution picture data, The 3rd step which acquires the same image data as the 1st aforementioned image data from other than the aforementioned record medium, performs transform processing to the data of the aforementioned frequency domain to the acquired image data, and obtains the 2nd resolution picture data, the difference which subtracted and obtained the resolution picture data of the above 2nd from the resolution picture data of the above 1st — the card type record-medium authentication technique characterized by consisting of the 4th step which compares ID information restored from data and the aforementioned card type record medium, and judges the justification of the aforementioned storage
[Claim 7] Transform processing to the data of the aforementioned frequency domain is the card type record-medium authentication technique according to claim 6 characterized by being Fourier transformation.
[Claim 8] Transform processing to the data of the aforementioned frequency domain is the card type record-medium authentication technique according to claim 6 characterized by being the discrete cosine conversion given to each of the block which divides the 1st aforementioned image data into plurality, and is acquired.
[Claim 9] the above with which the 4th aforementioned step was obtained for every aforementioned block — the difference — the claim 6 which compares ID information restored from data and the aforementioned card type record medium, and is characterized by making the aforementioned judgment by the majority of a comparison result, or the card type record-medium authentication technique given in 7 and 8
[Claim 10] It is a card type record medium containing the picture image field where the data area on which the data containing an owner's ID information were recorded, and image data are recorded. in the aforementioned picture image field Transform processing to the data of a frequency domain is performed to the 1st image data which specifies the owner itself. In the card type record-medium authentication equipment with which the 2nd image data generated by adding the aforementioned ID information to the data of the frequency domain after this conversion, and carrying out the inverse transformation of this added data to a picture signal is recorded ID information reading machine which restores the aforementioned ID information from the aforementioned card type record medium, The picture image reading machine which reads the data of the aforementioned picture image field, and the transform-processing section which performs transform processing to the data of a frequency domain to the data of the aforementioned picture image field, and generates the 1st resolution picture data, The 2nd picture image reading machine which reads the same image data as the 1st aforementioned image data in other than the aforementioned record medium, The 2nd transform-processing section which performs transform processing to the data of the aforementioned frequency domain to the acquired image data, and obtains the 2nd resolution picture data, the resolution picture data of the resolution picture data of the above 1st to the above 2nd — subtracting — the difference — with the subtractor which obtains data the above — the difference — the judgment circuit which compares ID information restored from data and the aforementioned card type record medium, and judges the justification of the aforementioned card type storage — ** — since — the card type record-medium authentication equipment characterized by becoming
[Claim 11] In the card type record-medium cipher system containing an encryption means to encipher ID information recorded on a magnetic card, and a magnetic information creation means to make a magnetic information enciphered ID information and to record on the aforementioned magnetic card A frequency-domain conversion means to change the subject-copy pattern of the pattern of the aforementioned magnetic card into the information on a frequency domain, An addition means to change ID information recorded on the aforementioned magnetic card into the conversion information distributed over the frequency

domain, and to add the aforementioned conversion information and the information generated by conversion by the aforementioned frequency-domain conversion means, A frequency-domain inverse-transformation means to return the information on the frequency domain generated by the addition by the aforementioned addition means to a two-dimensional picture image pattern, The card type record-medium cipher system characterized by having a picture image pattern printing means to print to the concerned magnetic card so that the picture image pattern generated by the aforementioned frequency-domain inverse-transformation means may be used as a pattern of the aforementioned magnetic card.

[Claim 12] The card type record-medium cipher system according to claim 11 characterized by having an addition means to make it similar to distribution **** of the subject-copy image frequency spectrum which is an information on the frequency domain generated by conversion by the aforementioned frequency-domain conversion means, to generate ID information frequency spectrum, and to add the concerned subject-copy image frequency spectrum and the concerned ID information frequency **********.

[Claim 13] The card type record-medium cipher system according to claim 11 or 12 characterized by for the aforementioned frequency-domain conversion means performing FFT, and a frequency-domain inverse-transformation means performing reverse FFT.

[Claim 14] The card type record-medium cipher system according to claim 11 or 12 characterized by for the aforementioned frequency-domain conversion means performing DCT, and a frequency-domain inverse-transformation means performing reverse DCT.

[Claim 15] In the card type record-medium decoder of the record medium which stenciled the picture image pattern containing enciphered ID information and ID information The magnetic read station which reads in the magnetic stripe of the aforementioned record medium ID information by which encryption was carried out [aforementioned], A frequency-domain conversion means to change the subject-copy pattern of the pattern of a magnetic card into the information on a frequency domain by the aforementioned magnetic head, A reverse encryption means to reverse-encipher ID information by which encryption was carried out [aforementioned], and to output ID information, A picture image reading means to read the aforementioned picture image pattern, and a frequency-domain conversion means to change the aforementioned picture image pattern into a frequency domain, the subtractor which deducts the data which changed the aforementioned ID information into the frequency domain from the data of the aforementioned frequency domain, and a frequency-domain inverse-transformation means to return the information on the frequency domain generated by subtraction by the aforementioned subtractor to a two-dimensional picture image pattern -- since -- the becoming card type record-medium decoder

[Claim 16] The card type record medium characterized by recording further the image data generated by carrying out the inverse transformation of the aforementioned spatial-frequency data with which the aforementioned identification data were embedded to a time data after embedding the identification data which are the card type record medium with which the specific data which specify an owner were written in, and were generated based on the aforementioned specific data in the spatial-frequency data of a photograph.

[Claim 17] It is the card type record medium according to claim 16 which the aforementioned spatial-frequency data are the photograph picture image by which dispersed cosine conversion was carried out, and is characterized by the aforementioned inverse transformation being reverse dispersed cosine conversion.

[Claim 18] the component to which, as for the aforementioned spatial-frequency data with which the aforementioned identification data were embedded, each component of the spatial-frequency data of the aforementioned photograph data and the aforementioned identification data correspond -- a multiplication -- carrying out -- this multiplication value -- constant twice -- the card type record medium according to claim 16 or 17 characterized by being data created by adding the value carried out to the component to which the spatial-frequency data of the aforementioned photograph data correspond

[Claim 19] The aforementioned specific data are a card type record medium given in the claim 16 characterized by being written in the magnetic-recording section, or any 1 term of 18.

[Claim 20] The card type record medium characterized by using a card type record medium given in the claim 16 or any 1 term of 18 for an identification card or a credit card.

[Claim 21] A means to generate identification data based on the specific data which specify an owner, The multiplication of a means to change into spatial-frequency data the photograph which should be stuck, and each component of the aforementioned spatial-frequency data and the component to which the aforementioned identification data correspond is carried out. this multiplication value -- constant twice -- with a means to add the value carried out to the component to which the spatial-frequency data of the aforementioned photograph data correspond, to carry out the inverse transformation of this added spatial-frequency data, and to change into image data The card type record-medium creation system characterized by having the means which writes the aforementioned image data and the aforementioned specific data in a card type record medium.

[Claim 22] It is the card type record-medium creation system according to claim 21 which the aforementioned conversion is dispersed cosine conversion and is characterized by the aforementioned inverse transformation being reverse dispersed cosine conversion.

[Claim 23] After embedding the identification data generated based on the specific data which specify an owner in the spatial-frequency data of a photograph It is the card type record-medium authentication equipment recorded with the aforementioned specific data in the image data generated by carrying out the inverse transformation of the aforementioned spatial-frequency data with which the aforementioned identification data were embedded to a time data. A means to generate the aforementioned identification data based on the aforementioned specific data, and a conversion means to change the aforementioned image data into the aforementioned spatial-frequency data, Card type record-medium authentication equipment equipped with a means to perform the correlation operation of the output of the aforementioned conversion means, and the aforementioned identification data, and to judge the truth or falsehood of a card type record medium based on this correlation result of an operation.

[Claim 24] The step which generates identification data based on the specific data which are the record medium which stored the program for operating a card type record-medium creation system in a computer, and specify an owner, The step which changes into spatial-frequency data the photograph picture image which should be stuck, The multiplication of each component of the aforementioned spatial-frequency data and the component to which the aforementioned identification data correspond is carried out. this multiplication value -- constant twice -- with the step which adds the value carried out to the component to which the spatial-frequency data of the aforementioned photograph picture image correspond, carries out the inverse transformation of this added spatial-frequency data, and is changed into image data The record medium characterized by storing the program containing the step which writes the aforementioned image data and the aforementioned specific data in a card type record medium.

[Claim 25] It is the record medium characterized by for the aforementioned conversion being dispersed cosine conversion and storing the program for operating in a computer the card type record-medium creation system according to claim 24 characterized by the aforementioned inverse transformation being reverse dispersed cosine conversion.
[Claim 26] After embedding the identification data generated based on the specific data which specify an owner in the spatial-frequency data of a photograph The image data generated by carrying out the inverse transformation of the aforementioned spatial-frequency data with which the aforementioned identification data were embedded to a time data The step which is the record medium which stored the program for operating in a computer the check system of the card type record medium recorded with the aforementioned specific data, and generates the aforementioned identification data based on the aforementioned specific data, The record medium characterized by storing the program containing the step which changes the aforementioned image data into spatial-frequency data, and the step which performs the correlation operation of this conversion result and the aforementioned identification data, and judges the truth or falsehood of a card type record medium based on this correlation result of an operation.
[Claim 27] In the card type record medium containing the picture image field where the data area on which the data containing ID information peculiar to an owner were recorded, and image data are recorded in the aforementioned picture image field Transform processing to the data of a frequency domain is performed to the 1st image data which specifies the owner itself. The card type record medium characterized by recording the 2nd image data generated by adding the data which changed the aforementioned ID information into the data of the frequency domain after this conversion at the frequency domain, and carrying out the inverse transformation of this added data to a picture signal.
[Claim 28] ID information on the aforementioned data area is a card type record medium according to claim 27 characterized by what is enciphered and recorded.
[Claim 29] The 1st aforementioned image data is a card type record medium according to claim 27 or 28 characterized by being an owner's fingerprint picture image or photograph-of-his-face picture image.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－275203

(43)公開日　平成10年(1998)10月13日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｔ
			Ｖ
Ｇ０６Ｔ　7/00		Ｇ０６Ｆ　15/62	４６０
Ｇ０６Ｋ　19/10		Ｇ０６Ｋ　19/00	Ｒ
19/06			Ｂ

審査請求　有　請求項の数29　ＯＬ　（全 20 頁）　最終頁に続く

(21)出願番号　特願平9－227979

(22)出願日　平成９年(1997)８月25日

(31)優先権主張番号　特願平8－317545
(32)優先日　平８(1996)11月28日
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平8－357504
(32)優先日　平８(1996)12月27日
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平9－20602
(32)優先日　平９(1997)２月３日
(33)優先権主張国　日本（ＪＰ）

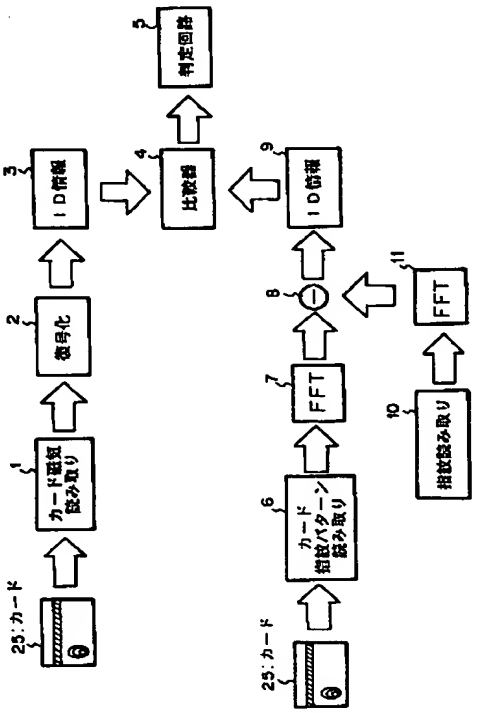
(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　高井　和人
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　藤原　司郎
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　弁理士　山下　穣平

(54)【発明の名称】　カード型記録媒体及びその認証方法及び認証装置、作成システム、暗号化方式、その解読器と記録媒体

(57)【要約】

【課題】　カード型記録媒体の偽造及び不正使用の困難なセキュリティを向上したカード型記録媒体を提供する。

【解決手段】予め磁気カードの上に磁気データと同一の情報を、本人の指紋パターンをフーリエ変換（ＦＦＴ）、又はＤＣＴ変換した周波数スペクトラムパターンに重ねて、そのパターンを逆ＦＦＴ変換して磁気カードに印刷しておく。また、磁気カードの模様の原画パターンを周波数ドメインの情報にＦＦＴ又はＤＣＴ変換し、当該磁気カードのＩＤ情報を周波数ドメインに分布させた情報を生成し、当該生成情報と変換された情報とを加算し、加算手段による加算によって生成された周波数ドメインの情報を２次元の画像パターンに戻し、生成された画像パターンを当該磁気カードの模様として使うように当該磁気カードに印刷する。また、身分証明書についても、顔写真に識別コードを埋め込み、正規の所有者と顔写真の所有者とが同一か否かを判定する。



【特許請求の範囲】

【請求項１】　所有者のＩＤ情報を含むデータが記録されたデータ領域と画像データが記録される画像領域とを含むカード型記録媒体において、

前記画像領域には、所有者自身を特定する第１の画像データに周波数領域のデータへの変換処理を施し、この変換後の周波数領域のデータに前記ＩＤ情報を加算し、この加算されたデータを画像信号に逆変換することにより生成された第２の画像データが記録されていることを特徴とするカード型記録媒体。

【請求項２】　前記データ領域のＩＤ情報は、暗号化されて記録されていることを特徴とする請求項１に記載のカード型記録媒体。

【請求項３】　前記第１の画像データは、所有者の指紋画像又は顔写真画像であることを特徴とする請求項１又は２に記載のカード型記録媒体。

【請求項４】　前記周波数領域のデータへの変換処理は、フーリエ変換であることを特徴とする請求項１又は２，３に記載のカード型記録媒体。

【請求項５】　前記周波数領域のデータへの変換処理は、前記第１の画像データを複数個に分割して得られるブロックの各々に施されるデイスクリートコサイン変換であることを特徴とする請求項１又は２，３に記載のカード型記録媒体。

【請求項６】　所有者のＩＤ情報を含むデータが記録されたデータ領域と画像データが記録される画像領域とを含むカード型記録媒体であり、前記画像領域には、所有者自身を特定する第１の画像データに周波数領域のデータへの変換処理を施し、この変換後の周波数領域のデータに前記ＩＤ情報を加算し、この加算されたデータを画像信号に逆変換することにより生成された第２の画像データが記録されているカード型記録媒体認証方法であり、

前記カード型記録媒体から前記ＩＤ情報を復元するとともに、前記画像領域のデータを読み取る第１のステップと、

前記画像領域のデータに周波数領域のデータへの変換処理を施して第１の変換画像データを生成する第２のステップと、

前記第１の画像データと同じ画像データを前記記録媒体以外から取得し、取得した画像データに前記周波数領域のデータへの変換処理を施して第２の変換画像データを得る第３のステップと、

前記第１の変換画像データから前記第２の変換画像データを減算して得た差分データと前記カード型記録媒体から復元されたＩＤ情報とを比較し、前記記憶媒体の正当性を判断する第４のステップ、とからなることを特徴とするカード型記録媒体認証方法。

【請求項７】　前記周波数領域のデータへの変換処理は、フーリエ変換であることを特徴とする請求項６に記載のカード型記録媒体認証方法。

【請求項８】　前記周波数領域のデータへの変換処理は、前記第１の画像データを複数個に分割して得られるブロックの各々に施されるデイスクリートコサイン変換であることを特徴とする請求項６に記載のカード型記録媒体認証方法。

【請求項９】　前記第４のステップは、前記ブロック毎に得られた前記差分データと前記カード型記録媒体から復元されたＩＤ情報とを比較し、比較結果の多数決により、前記判断を行うことを特徴とする請求項６又は７，８に記載のカード型記録媒体認証方法。

【請求項１０】　所有者のＩＤ情報を含むデータが記録されたデータ領域と画像データが記録される画像領域とを含むカード型記録媒体であり、前記画像領域には、所有者自身を特定する第１の画像データに周波数領域のデータへの変換処理を施し、この変換後の周波数領域のデータに前記ＩＤ情報を加算し、この加算されたデータを画像信号に逆変換することにより生成された第２の画像データが記録されているカード型記録媒体認証装置において、

前記カード型記録媒体から前記ＩＤ情報を復元するＩＤ情報読取器と、

前記画像領域のデータを読み取る画像読取器と、

前記画像領域のデータに周波数領域のデータへの変換処理を施して第１の変換画像データを生成する変換処理部と、

前記第１の画像データと同じ画像データを前記記録媒体以外から読取る第２の画像読取器と、

取得した画像データに前記周波数領域のデータへの変換処理を施して第２の変換画像データを得る第２の変換処理部と、

前記第１の変換画像データから前記第２の変換画像データを減算して差分データを得る減算器と、

前記差分データと前記カード型記録媒体から復元されたＩＤ情報とを比較して前記カード型記憶媒体の正当性を判断する判定回路と、とからなることを特徴とするカード型記録媒体認証装置。

【請求項１１】　磁気カードに記録するＩＤ情報を暗号化する暗号化手段と、暗号化されたＩＤ情報を磁気情報として前記磁気カードに記録する磁気情報作成手段とを含むカード型記録媒体暗号化方式において、

前記磁気カードの模様の原画パターンを周波数ドメインの情報に変換する周波数ドメイン変換手段と、

前記磁気カードに記録するＩＤ情報を周波数ドメインに分布させた変換情報に変換し、前記変換情報と前記周波数ドメイン変換手段による変換によって生成された情報とを加算する加算手段と、

前記加算手段による加算によって生成された周波数ドメインの情報を２次元の画像パターンに戻す周波数ドメイン逆変換手段と、

前記周波数ドメイン逆変換手段によって生成された画像パターンを前記磁気カードの模様として使うように当該磁気カードに印刷する画像パターン印刷手段とを有することを特徴とするカード型記録媒体暗号化方式。

【請求項１２】　前記周波数ドメイン変換手段による変換によって生成された周波数ドメインの情報である原画像周波数スペクトラムの分布伏態に類似させてＩＤ情報周波数スペクトラムを生成して当該原画像周波数スペクトラムと当該ＩＤ情報周波数スペクトラムとを加算する加算手段とを有することを特徴とする請求項１１に記載のカード型記録媒体暗号化方式。

【請求項１３】　前記周波数ドメイン変換手段がＦＦＴを行い、周波数ドメイン逆変換手段が逆ＦＦＴを行うことを特徴とする請求項１１又は１２に記載のカード型記録媒体暗号化方式。

【請求項１４】　前記周波数ドメイン変換手段がＤＣＴを行い、周波数ドメイン逆変換手段が逆ＤＣＴを行うことを特徴とする請求項１１又は１２に記載のカード型記録媒体暗号化方式。

【請求項１５】　暗号化されたＩＤ情報と、ＩＤ情報を含む画像パターンを刷り込んだ記録媒体のカード型記録媒体解読器において、

前記記録媒体の磁気ストライプから前記暗号化されたＩＤ情報を読み取る磁気読取部と、

前記磁気ヘッドで磁気カードの模様の原画パターンを周波数ドメインの情報に変換する周波数ドメイン変換手段と、

前記暗号化されたＩＤ情報を逆暗号化してＩＤ情報を出力する逆暗号化手段と、

前記画像パターンを読み取る画像読取手段と、

前記画像パターンを周波数ドメインに変換する周波数ドメイン変換手段と、

前記周波数ドメインのデータから前記ＩＤ情報を周波数ドメインに変換したデータを差し引く減算器と、前記減算器による減算によって生成された周波数ドメインの情報を２次元の画像パターンに戻す周波数ドメイン逆変換手段と、からなるカード型記録媒体解読器。

【請求項１６】　所有者を特定する特定データが書き込まれたカード型記録媒体であって、

前記特定データに基づいて生成された識別データを、写真の空間周波数データ内に埋め込んだ後に、前記識別データが埋め込まれた前記空間周波数データを時間データに逆変換することにより生成された画像データを更に記録していることを特徴とするカード型記録媒体。

【請求項１７】　前記空間周波数データは、離散的コサイン変換された写真画像であり、前記逆変換は、逆離散的コサイン変換であることを特徴とする請求項１６に記載のカード型記録媒体。

【請求項１８】　前記識別データが埋め込まれた前記空間周波数データは、前記写真データの空間周波数データの各成分と前記識別データの対応する成分とを乗算し、この乗算値を定数倍した値を、前記写真データの空間周波数データの対応する成分に加算することにより作成されたデータであることを特徴とする請求項１６又は１７に記載のカード型記録媒体。

【請求項１９】　前記特定データは、磁気記録部に書き込まれていることを特徴とする請求項１６乃至１８のいずれか１項に記載のカード型記録媒体。

【請求項２０】　請求項１６乃至１８のいずれか１項に記載のカード型記録媒体を身分証明書又はクレジットカードに用いることを特徴とするカード型記録媒体。

【請求項２１】　所有者を特定する特定データに基づいて識別データを生成する手段と、

貼付されるべき写真を、空間周波数データに変換する手段と、

前記空間周波数データの各成分と前記識別データの対応する成分とを乗算し、この乗算値を定数倍した値を前記写真データの空間周波数データの対応する成分に加算し、この加算された空間周波数データを逆変換して画像データに変換する手段と、

前記画像データと前記特定データとをカード型記録媒体に書き込む手段とを備えたことを特徴とするカード型記録媒体作成システム。

【請求項２２】　前記変換は離散的コサイン変換であり、前記逆変換は逆離散的コサイン変換であることを特徴とする請求項２１に記載のカード型記録媒体作成システム。

【請求項２３】　所有者を特定する特定データに基づいて生成された識別データを、写真の空間周波数データ内に埋め込んだ後に、前記識別データが埋め込まれた前記空間周波数データを時間データに逆変換することにより生成された画像データを前記特定データとともに記録されたカード型記録媒体認証装置であって、

前記特定データに基づいて前記識別データを生成する手段と、

前記画像データを前記空間周波数データに変換する変換手段と、

前記変換手段の出力と前記識別データとの相関演算を行い、この相関演算結果に基づいてカード型記録媒体の真贋を判定する手段とを備えたカード型記録媒体認証装置。

【請求項２４】　カード型記録媒体作成システムを電子計算機で動作させるためのプログラムを格納した記録媒体であり、

所有者を特定する特定データに基づいて識別データを生成するステップと、

貼付されるべき写真画像を、空間周波数データに変換するステップと、

前記空間周波数データの各成分と前記識別データの対応する成分とを乗算し、この乗算値を定数倍した値を前記

写真画像の空間周波数データの対応する成分に加算し、この加算された空間周波数データを逆変換して画像データに変換するステップと、
前記画像データと前記特定データとをカード型記録媒体に書き込むステップとを含むプログラムを格納したことを特徴とする記録媒体。
【請求項２５】　前記変換は離散的コサイン変換であり、前記逆変換は逆離散的コサイン変換であることを特徴とする請求項２４に記載のカード型記録媒体作成システムを電子計算機で動作させるためのプログラムを格納したことを特徴とする記録媒体。
【請求項２６】　所有者を特定する特定データに基づいて生成された識別データを、写真の空間周波数データ内に埋め込んだ後に、前記識別データが埋め込まれた前記空間周波数データを時間データに逆変換することにより生成された画像データが、前記特定データとともに記録されたカード型記録媒体の検査システムを電子計算機で動作させるためのプログラムを格納した記録媒体であり、
前記特定データに基づいて前記識別データを生成するステップと、
前記画像データを空間周波数データに変換するステップと、
この変換結果と前記識別データとの相関演算を行い、この相関演算結果に基づいてカード型記録媒体の真贋を判定するステップとを含むプログラムを格納したことを特徴とする記録媒体。
【請求項２７】　所有者固有のＩＤ情報を含むデータが記録されたデータ領域と画像データが記録される画像領域とを含むカード型記録媒体において、
前記画像領域には、所有者自体を特定する第１の画像データに周波数領域のデータへの変換処理を施し、この変換後の周波数領域のデータに前記ＩＤ情報を周波数領域に変換したデータを加算し、この加算されたデータを画像信号に逆変換することにより生成された第２の画像データが記録されていることを特徴とするカード型記録媒体。
【請求項２８】　前記データ領域のＩＤ情報は、暗号化されて記録されていることを特徴とする請求項２７に記載のカード型記録媒体。
【請求項２９】　前記第１の画像データは、所有者の指紋画像又は顔写真画像であることを特徴とする請求項２７又は２８に記載のカード型記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、クレジットカードやキャッシュカード、身分証明書等の磁気カードを含むカード型記録媒体に関し、特にそのカード型記録媒体の正当性を検証する認証方法、磁気カードに記録されるＩＤ(IDentification) 情報の暗号化を行うカード型記録媒体暗号化方式、文字化された個人データと共に本人の顔写真が記録されたカード型記録媒体、さらに当該カード型記録媒体の作成方法や解読方法をコンピュータのプログラムとして記録した記録媒体に関する。
【０００２】
【従来の技術】従来、クレジットカードやキャッシュカードの様な磁気カードの正当な所有者を検証する技術や磁気カードＩＤ情報暗号化方式としては、たとえば特開昭６４－７６２７０号公報に示されるように、クレジットカードやキャッシュカードとして使用される磁気カードにおいて、当該磁気カードの所有者を確認する際のセキュリティを向上させるために、当該磁気カードに記録しておきたい磁気情報としてのＩＤ情報と引き出し金額等の価値情報等の暗号化を行い、また磁気カードに暗号化された所有者のＩＤ情報が記憶され、磁気カードからＩＤ情報を復号し、所有者が別途入力するＩＤ情報と比較することにより、そのカードの正当な所有者であることを検証している（以下、「第１の従来技術」）。
【０００３】図２０は、従来の磁気カードＩＤ情報暗号化方式の一例の構成を示すブロック図である。以下に、図２０を参照して、従来の磁気カードＩＤ情報暗号化方式の動作を説明する。暗号化手段７２は、磁気カードのＩＤ情報７１の磁気情報を読み込んだだけでは容易に当該ＩＤ情報のデータの分析ができないように、当該ＩＤ情報７１の暗号化を行う（暗号化の態様としては様々なものが存在する）。磁気情報作成手段７３は、暗号化手段７２によって生成された磁気情報（暗号化されたＩＤ情報）を磁気カード上の磁気記録部分（磁気ストライプ等）に記録する。
【０００４】また、特開平０６－１３５１８７号公報は、カード本来が記憶している磁気データ以外に、所有者の顔写真をカードに印刷され、また写真情報を暗号化したデータも印刷された磁気カードを開示している。この公報記載の技術では、カードの保有者の外観情報を表示した画像領域と、該画像情報を所定のロジックに基づき変換した暗号情報を表示したスクランブル領域とを備え、その暗号化した写真情報を逆ロジックで復号し、顔写真の画像情報との同一性を照合され、カードの正当性を機械的に判別している（以下、「第２の従来技術」）。
【０００５】更に近年、写真付きの身分証明書が普及している。パスポート、民間企業の社員証、各種免許証などがそうである。またクレジットカードにも写真の貼られたものが普及しつつあり、これらを総称して「身分証明書」と称する。特に公的機関が発行したもので、写真が貼られているものは身分の確認に利用されている。しかし、これらの身分証明書は偽造されることがある。現実に、写真を刷り込み印刷することで、偽造しにくくしたはずの現在の小型のパスポートでも、すでに写真のみを貼りかえた偽造パスポートが出ている。しかも、この

偽造パスポートは非常に精巧にできており、偽造と見破るのがかなり困難なものになっている。

【０００６】この偽造パスポートを含め偽造身分証明書ができる理由は、次の２つがあげられる。（１）写真を貼りかえることができる。（２）写真と身分証明書に記載されている項目とに関連がまったくない。いいかえれば、写真のみ貼りかえて他の記載事項を変更しなくても、その身分証明書は、一見しただけでは真正のものか、偽造のものかを判別できない。

【０００７】これを防ぐには、（ａ）偽造行為そのものが困難なように身分証明書を作成する方法、（ｂ）偽造されたとしても、その身分証明書が偽造であることを判別することで、偽造身分証明書の使用を防止する方法が必要となる。

【０００８】ここで、（ａ）の方法の一例が、特開平３－１９３４９５号公報に示されている（以下、「第３の従来技術」）。この公報では、顔写真情報や属性情報、レイアウト情報等を取り込んだ画像処理装置を用いたＩＤカード発行システムにおいて、前記情報に加えて偽造防止情報をも画像処理してイメージパターンとし、複雑なパタンを写真の上に重ね合わせ、その重ね合わせた写真を身分証明書に印刷する方法をとっている。この方法で写真に重ね合わせるパターンを複雑にすることで、偽造を防止する効果をねらっている。

【０００９】また、（ｂ）の方法としては、特開平３－１８５５８５号公報の第５の実施例に示されたものがある（以下、「第４の従来技術」）。この例では、身分証明書に記載されているデータに基づいて、真正身分証明書か、偽造身分証明書かを判別する為の識別データを作成し、それを身分証明書の写真部分に重ね合わせて印刷する方法をとっている。この方法であれば、身分証明書の記載事項と写真に重ね合わされている識別データとを照合できるため、写真を貼りかえられたとしても、偽造を見抜くことができる。

【００１０】また、この特開平３－１８５５８５号公報には、写真の中にこの識別データを埋め込んでしまう方法も記載されている。記載事項から計算によって識別データを求め、これを写真の一部分に埋め込むことにより実現している。

【００１１】別の観点からすると、身分証明書に印刷されている写真が正規のものであることが判別されれば、偽造であることを判別することができる。そこで、画像を周波数変換し、周波数スペクトラムに電子透かし（Digital Watermark）データを埋め込む方法が提案されている（日経エレクトロニクス　１９９６．４．２２（Ｎｏ．６６０）　１３ページ，同誌１９９７．２．２４（Ｎｏ．６８３）　９９－１２４ページ）（以下、「第５の従来技術」）。この方法においては、オリジナル作品をＤＣＴや高速フーリエ変換で周波数変換し、周波数スペクトラムにユーザ毎に固有の乱数のＩＤ情報を加えてスペクトラム拡散する。このＩＤ情報を含む周波数スペクトラムを逆周波数変換して、ＩＤ情報を隠し持つ周波数スペクトラムとオリジナル作品の周波数スペクトラムとの差分を取ればＩＤ情報が生成されるので、このＩＤ情報を正規のＩＤ情報とを比較すれば、正規に購入したオリジナル作品であるのか否かを判断することができる。このＩＤ情報を低域周波数成分の周波数スペクトラムとして、周波数成分に電子すかしデータを埋め込むので、圧縮処理やフィルタリング等の画像処理に対しても電子すかしデータが失われることはない。さらに、電子すかしデータとして正規分布に従う乱数を採用することで、電子すかしデータ同士の干渉を防ぎ、画質に大きな影響を及ぼすことなく電子すかしデータを破壊することを困難にしている。

【００１２】この電子すかしデータの埋め込み方法は、次のとおりである。まず、元の画像を離散コサイン（ＤＣＴ）変換などを用いて周波数成分に変換し、周波数領域で高い値を示すデータをｎ個選び、

ｆ（１），ｆ（２），…，ｆ（ｎ）

とする。次に電子すかしデータ

ｗ（１），ｗ（２），…，ｗ（ｎ）

を平均０分散１である正規分布より選び、

Ｆ（ｉ）＝ｆ（ｉ）＋α｜ｆ（ｉ）｜＊ｗ（ｉ）

を各周波数成分ｉについて計算する。ここでαはスケーリング要素である。最後にｆ（ｉ）の変わりにＦ（ｉ）を置き換えた周波数成分に逆離散コサイン変換を施し、電子すかしデータが埋め込まれた画像を得る。

【００１３】電子すかしデータの検出は以下の方法で行う。この検出方法においては、元の画像、及び電子すかしデータ候補ｗ（ｉ）（但しｉ＝１，２，…，ｎ）が既知でなければならない。

【００１４】まず、電子すかしデータ入り画像をＤＣＴ等を用いて周波数成分に変換する。次に、ｆ（ｉ）及びＦ（ｉ）により、電子すかしデータＷ（ｉ）を

Ｗ（ｉ）＝（Ｆ（ｉ）－ｆ（ｉ））／ｆ（ｉ）

により計算して抽出する。次にｗ（ｉ）とＷ（ｉ）の統計的類似度をベクトルの内積を利用して、

Ｃ＝Ｗ＊ｗ／（ＷＤ＊ｗＤ）

により計算する。ここで、

Ｗ＝（Ｗ（１），Ｗ（２），…，Ｗ（ｎ））、

ｗ＝（（１），ｗ（２），…，ｗ（ｎ））、

（但し、ＷＤ＝ベクトルＷの絶対値、ｗＤ＝ベクトルｗの絶対値）である。

【００１５】統計的類似度Ｃがある特定の値以上である場合には該当電子すかしデータが埋め込まれていると判定する。

【００１６】この電子すかしを、身分証明書の記載事項から生成し、印刷する写真に埋め込む。検査の時に写真からこの電子すかしを取り出して、記載事項と比較することで、身分証明書が真正か偽造か判別することが可能

である。

【００１７】

【発明が解決しようとする課題】上記第１の従来技術では、磁気カードの磁気情報を読み込んで、その磁気情報を当該磁気カード上の磁気記録部分と同じように他の磁気カード上の磁気記録部分に書き込むだけで、同一の磁気カード（同一とみなされる磁気カード）を作ることができるので、容易に第三者が磁気情報をそのまま複製すれば、同一のカードを作成することができる。また、図２０に示すような従来の磁気カードＩＤ情報暗号化方式においては、磁気カードのＩＤ情報を磁気情報として記録しているだけであるので、第三者が容易に当該磁気カードの複製を行うことができる。

【００１８】また、カードに写真等が貼る第２の従来技術でも、そのままコピーすれば、同一のカードが作れる。また顔写真と相関の有るデータが印刷されているので、カードの写真データを元に内容を解析され易い。また、この従来技術２では、カードの写真部や暗号化した写真情報部に大きな傷が入ると、真正のカードを偽造カードと誤認してしまう可能性がある。すなわち、写真情報を暗号化したデータを磁気カードに印刷するという従来の方式では、そのままその印刷データをコピーすれば同一の磁気カードを作ることができ、顔写真と相関のあるデータが「写真情報を暗号化したデータ」として印刷されているために、磁気カード上の顔写真を基にそのＩＤ情報（写真情報を暗号化したデータ）の内容を解析され易いという問題点がある。

【００１９】さらに、第３の従来技術では、偽造防止用の情報が偽造しようとする者に見えるため、そこの重ね合わされている複雑なパタンを模倣して、通常の人がみる限りでは偽造かどうか判別できないレベルにもっていくことができる。今日の写真技術、画像処理技術、印刷技術のレベルを考えるとこの偽造防止用のパタンを模倣することは可能である。その結果、身分証明書の記載事項に明白な間違い、例えば、正規の社員番号と桁数が相違、本来はアラビア数字でなければならない社員番号が漢数字になっているなどがない限り、偽造身分証明書を見分けることは難しい。

【００２０】また、第４の従来技術では、身分証明書の記載事項から生成した識別データを写真のうえに重ね合わせる形で印刷している。この方法であれば真正か偽造かを判断することができる。しかし、この場合は記載事項と識別するデータが可視データとなっているため、充分な数のデータを集積すれば、記載事項から識別するデータを生成する計算式を両データから逆算にて導くことが可能となってくる。この計算式が見出されてしまうと当該身分証明書と同じ計算式を用いた身分証明書は、無制限に偽造されることになる。また、写真の中にこの識別データを埋め込んでしまう方法も記載されているが、この実施例では識別データが埋め込まれている位置を固定しているため、偽造する者からすれば位置を特定しやすい。

【００２１】また、第５の従来技術による電子すかしを利用する場合は、元の写真が必要であり、身分証明書とともにこの元の写真をもっていることは通常ありえない。従って、この技術だけで身分証明書の持ち主が正規の持ち主か否かを判断することは困難である。

【００２２】本発明の目的は、磁気カードに入れる情報を、磁気データとカードの模様の両方に持たせて、容易に第３者がカードの複製を出来ない様にし、もし複製した場合は容易に判別出来る様にして、セキュリティを向上させることを目的とする。

【００２３】また、本発明の目的は、磁気カードに記録／印刷するＩＤ情報を、磁気情報の形態と磁気カードの模様に埋め込む形態との両方の形態で持たせて、第三者が容易に磁気カードの複製をできないようにして、磁気カードに関するセキュリティを向上させることができる磁気カードＩＤ情報暗号化方式を提供することにある。

【００２４】さらに、本発明の目的は、上記電子すかし技術を利用して、身分証明書の偽造を極めて困難として、たとえ偽造したとしても、簡単に正規の持ち主か否かを判別できることを目的とする。

【００２５】

【課題を解決するための手段】本発明の磁気カードの暗号解読方式は、第３者がカードの磁気を不正に複製した場合に、容易に複製したカードであるか判断が出来る様に、磁気データの他にカードの模様に情報を入れる手段を設けることにより、不正な複製かどうかを容易に判断する手段を提供する。

【００２６】より具体的には、予めオリジナルのカードの模様には、カードの模様の元になる所有者の指紋パターンをＦＦＴ（高速フーリエ変換）処理を施こして周波数ドメインの情報に変換し、ＩＤ情報を、この周波数ドメインの情報でエネルギーの強い周波数成分に加算し、その加算した結果を逆ＦＦＴ処理で周波数ドメインから２次元の画像イメージに変換して、カードにＩＤ情報が埋めこまれている指紋パターンの模様を印刷しておく。

【００２７】このカードの指紋パターンを読み取り機で読み込み、その画像をＦＦＴ処理で周波数ドメインの情報に変換し、所有者の指紋を読み取り機で読み取り、そのデータにＦＦＴ処理を施して周波数ドメインの情報に変換したものとの差分を取り、ＩＤ情報を抽出する。

【００２８】また、今まで通りカード磁気読み取り機で読み込まれたデータを、復号化して解読しＩＤ情報を抽出する。このＩＤ情報とカード模様から抽出したＩＤ情報とを比較し、同じＩＤで有ればオリジナルのカードで有り、違うＩＤで有れば不正に複製したカードであると判断する。

【００２９】本発明の磁気カードには、通常の磁気情報の他に、カードの模様にもＩＤ情報を入れている。この

ため、磁気データだけを複製しても模様部分を複製しない限り、同一カードとして見なされない。カードの模様から抽出したＩＤ情報と磁気データから抽出したＩＤ情報を比較することによって、容易にカードの不正な複製を見分けることが可能となる。また、模様にＩＤ情報が入っていることは、模様の周波数成分のエネルギーの強いところにＩＤ情報が刷り込まれる為、素人が見分けることは不可能となる。もし仮に、模様の違いが分かったとしても、本人の指紋パターンが無い限り、ＩＤ情報を抽出することは不可能である。

【００３０】さらに、本発明の磁気カードＩＤ情報暗号化方式は、磁気カードのＩＤ情報を暗号化する暗号化手段と、暗号化されたＩＤ情報を磁気情報として当該磁気カードに記録する磁気情報作成手段とを含む磁気カードＩＤ情報暗号化方式において、磁気カードの模様の原画パターンを周波数（空間周波数）ドメインの情報に変換する周波数ドメイン変換手段と、当該磁気カードのＩＤ情報を周波数ドメインに分布させた情報を生成し、当該生成された情報と前記周波数ドメイン変換手段による変換によって生成された情報とを加算する加算手段と、前記加算手段による加算によって生成された周波数ドメインの情報を２次元の画像パターンに戻す周波数ドメイン逆変換手段と、前記周波数ドメイン逆変換手段によって生成された画像パターンを当該磁気カードの模様として使うように当該磁気カードに印刷する画像パターン印刷手段とを有することを特徴とする。ここで、周波数ドメイン変換手段はＦＦＴ（Fast Fourier Transform：高速フーリエ変換）手段またはＤＣＴ（Discrete Cosine Transform：離散コサイン変換）手段等によって実現され、周波数ドメイン逆変換手段は逆ＦＦＴ手段や逆ＤＣＴ手段等によって実現される。

【００３１】さらにまた、本発明によるカード型記録媒体は、カードに印刷する写真をデジタルデータとして取り込み、取り込んだデータをＤＣＴ変換をかけて空間周波数に変換し、変換後のデータに当該カードに記載されている事項から生成した識別データに挿入する。当該カードを身分証明書として使用した場合、該身分証明書に挿入されたデータをＩＤＣＴ変換をかけて通常の写真にもどし、身分証明書に記載されるデータとともに身分証明書に印刷する。検査する際には、身分証明書の写真、記載事項を読み込んで、読み込んだ写真のデータにＤＣＴをかけて空間周波数に変換し、一方、読み込んだ記載事項からは識別データを生成し、両者の相関関係から身分証明書が真正か偽造かを判断する。

【００３２】上記の構成をとっているので、身分証明書の写真と識別データ間の相関関係が強い場合は、当該身分証明書は真正であると判断する。また、相関関係が弱い場合は、当該身分証明書は偽造であると判断する。

【００３３】更に加えて、本発明は、カード型記録媒体作成システムを電子計算機で動作させるためのプログラムを格納した記録媒体であり、所有者を特定する特定データに基づいて識別データを生成するステップと、貼付されるべき写真画像を、空間周波数データに変換するステップと、前記空間周波数データの各成分と前記識別データの対応する成分とを乗算し、この乗算値を定数倍した値を前記写真画像の空間周波数データの対応する成分に加算し、この加算された空間周波数データを逆変換して画像データに変換するステップと、前記画像データと前記特定データとをカード型記録媒体に書き込むステップとを含むプログラムを格納したことを特徴とする。当該記録媒体には、各ステップ毎に記録媒体に書き込む画像領域とＩＤ情報や特定データを書き込むデータ領域にそれぞれ書き込むデータを作成するので、当該記録媒体の作成の容易性や、誤りのない統一的なカードが作成できる。

【００３４】

【発明の実施の形態】まず、本発明を実施するための最良の形態について図面を参照して詳細に説明する。

【００３５】［第１の実施形態］本発明による第１の実施形態について説明する。図１を参照すると、カード２５に書き込んでいるカード上の書込指紋パターンをカード画像読み取り機６で読み込み、その画像をＦＦＴ７で高速フーリエ変換する。一方現在の所持者である自分の指紋パターンを指紋パターン読み取り機１０で読み込み、そのデータをＦＦＴ１１で高速フーリエ変換する。減算器８は、ＦＦＴ７出力からＦＦＴ１１出力を減算し、ユーザを特定するＩＤ情報９を抽出する。

【００３６】また、カード２５の磁気データをカード磁気読み取り機１で読み取り、そのデータを復号化処理２によって符号を解読し、ＩＤ情報３を抽出する。

【００３７】これらのカード２５の模様から抽出したＩＤ情報９と磁気データから抽出したＩＤ情報３とを、比較器４で比較し、その比較結果により、不正に複製したものかどうかを判定回路５が判断する。

【００３８】次に、このカード２５の作成方法について説明する。このカード２５では、図３に示すように、指紋パターン１９と磁気ストライプ１８が作成されている。このカード２５には、カード２５の指紋パターンに予めＩＤ情報を埋めこんで置く。図２を用いて詳細にＩＤ情報の埋めこみ方法について説明する。

【００３９】図２において、カード２５に印刷する自分の指紋パターン１２を、不図示の画像読取装置によって指紋画像信号として読み出し、ＦＦＴ１１で高速フーリエ変換して周波数ドメインに変換して、ＩＤ情報９を周波数成分が強い帯域に加算器１３で加算する。この場合、強いエネルギーのところに微小なＩＤ情報を加算するので、原画像に対しては殆ど影響を与えない。

【００４０】次に、その結果を逆ＦＦＴ１４で２次元の画像イメージに変換して、カード２５に印刷する模様を作り、指紋パターン印刷機１５でカード２５に、図３に

示す符号１９のように指紋パターンを印刷する。ここで、印刷された指紋パターン１９は、見た目では自分の指紋パターン１２と区別が出来ない位の画像になり、この模様はＩＤ情報が異なっても同じ様に見える。

【００４１】また、ＩＤ情報９を、暗号化器１６で暗号化し、磁気テープ作成機１７でカードの磁気ストライプ（図３の１８）に磁気情報を作成する。この際、指紋パターン１９を書き込むステップと、磁気ストライプへの磁気情報を書き込むステップはいずれを先に行ってもよいが、一体的にマッチさせておく。

【００４２】以上の方法で、カードのＩＤ情報が、磁気データとカードの指紋パターンの模様の両方に刷り込まれたカードが出来る。

【００４３】図１に戻って、上述した方法で作成されたカード２５を、先ず、カードの模様を指紋パターン読み取り機６で読み込み、読み込んだ画像をＦＦＴ７で高速フーリエ変換して周波数ドメインの情報に変換する。ここで高速フーリエ変換は離散的数値系列のフーリエ変換であり、一般のフーリエ変換に対して計算回数を大幅に短縮できる変換方法である。この高速フーリエ変換をすると、指紋パターン＋ＩＤ情報の周波数スペクトラムが生成されるが、このスペクトラムは、図４の指紋データスペクトラム＋ＩＤ情報２０のように示される。次に、図１の指紋読み取り機１０で読みとられた所有者の指紋パターン１２をＦＦＴ１１で同様に周波数ドメインに変換すると、図４の符号２２に示されるような指紋データ周波数スペクトラム２２が得られる。減算器８で、指紋パターン＋ＩＤ情報の周波数スペクトラム２０から、指紋データ周波数スペクトラム２２を減算すると、ＩＤ情報の周波数スペクトラム２１に示される様に、ＩＤ情報の部分だけ抽出される。

【００４４】また、カード２５のカード磁気読み取り機１で、磁気データを読み出し、この情報を復号化処理２で符号を解読し、ＩＤ情報３を抽出する。カード磁気読み取り機１は、カード２５内の指紋パターンを光ヘッドの光電変換手段によって、カード２５内の磁気ストライプの磁気情報を磁気ヘッドの磁気／電気変換手段によって、カードと各ヘッドとを相対的に移動して、同時に又は個別に電気信号として読み出すことができる。

【００４５】次に、カード２５の指紋パターン１９の模様から抽出したＩＤ情報９とカードの磁気データから抽出したＩＤ情報３を比較器４で比較し、判定回路５において、同一のＩＤ情報であればそのカードは正規のカードと判定し、異なるＩＤ情報であればそのカードは不正に複製したカードと判定する。

【００４６】なお、以上の処理は、プログラムを格納したコンピュータ等によって実現できる。すなわち、以上の処理を実行するプログラムを、フロッピーディスク等の記憶媒体に格納させ、この記憶媒体からプログラムをロードしたコンピュータに実行させることもできる。

【００４７】また、上記実施形態では、指紋パターンとＩＤ情報とをカード型記録媒体に書き込んだ例を示したが、顔写真や目の網膜網等の特徴のある画像とＩＤ情報とをペアーとして扱うことで、カード型記録媒体の所持者を正当な所持者と判断でき、カード型記録媒体の偽造を防止し、偽物対策にも有効である。

【００４８】また、上記実施形態では、ＩＤ情報を磁気ストライプに記録する例を示したが、磁気カードばかりでなく、ＩＣカードであっても良く、例えばＩＤ情報をＥＥＰＲＯＭやフラッシュメモリ等に格納して上述の作用を適用してもよく、更に他のカード型記録媒体でも同様である。この点は、下記の実施形態でも適時適用できることは勿論である。

【００４９】［第２の実施形態］次に、本発明の第２の実施形態について図面を参照して詳細に説明する。なお、本実施形態は、第１の実施形態に従って、更に詳細に且つ具体的に説明するものである。図１を参照すると、カード２５の指紋パターン１９をカード画像読み取り機６で読み込む。ＦＦＴ７とＦＦＴ１１は、２５ポイントの周波数帯域に分ける高速フーリエ変換で、各周波数帯域当たりの量子化数は１６ビットとする。このＦＦＴ７でカードから読み取った指紋パターン１９を高速フーリエ変換したものから、指紋読み取り機１０で読み取った自分の指紋パターンをＦＦＴ１１で高速フーリエ変換したものを、減算器８で減算し、３２ビットのユーザを特定するＩＤ情報９を抽出する。

【００５０】また、カード２５の磁気データ１８をカード磁気読み取り機１で読み取り、そのデータを復号化２によって符号を解読し、３２ビットのＩＤ情報３を抽出する。

【００５１】これらのカード２５の指紋パターン１９の模様から抽出した３２ビットのＩＤ情報９と、磁気データ１８から抽出した３２ビットのＩＤ情報３を、比較器４で比較し、同一の時は”０”を出力し、異なる時は”１”を出力して、判定回路５において、”０”の時は正規のカードで、”１”の時は不正に複製したカードであると判定する手段により構成される。

【００５２】先ず、カード２５の指紋パターン１９の模様に予め３２ビットのＩＤ情報を埋めこんで置く。図２を用いて詳細にＩＤ情報の埋めこみ方法について説明する。カードに印刷する自分の指紋パターン１２を、ＦＦＴ１１で周波数ドメインに変換して、３２ビットのＩＤ情報９を周波数成分が強い帯域に加算器１２で加算する。ＦＦＴ１１は、２５ポイントの周波数帯域に分ける高速フーリエ変換で、各周波数帯域当たりの量子化数は１６ビットとする。この場合、強いエネルギーのところに微小なＩＤ情報を加算するので、自分の指紋パターンに対しては殆ど影響を与えない。この時の加算の方法は、３２ビットのＩＤ情報を４ビット×３ケ、３ビット×４ケ、２ビット×４ケに分けて、原画像の周波数成分

のエネルギーの強いところから順番に加算していく。次に、その結果を逆ＦＦＴ１４で２次元の画像イメージに変換して、カードに印刷する模様を作り、指紋パターン印刷機１５でカードに指紋パターンを印刷する。ここで、印刷された画像イメージは、見た目では自分の指紋パターン１２と区別が出来ない位の画像になり、この模様はＩＤ情報が異なっても全て同じ様に見える。

【００５３】また、３２ビットのＩＤ情報９を、暗号化器１６で暗号化し、磁気テープ作成機１７でカード２５に磁気情報を作成する。

【００５４】以上の方法で、３２ビットのＩＤ情報９が、磁気データ１８とカードの指紋パターン１９の模様の両方に刷り込まれたカードが出来る。

【００５５】上述した方法で作成したカード２５を、先ず、カード２５の指紋パターン１９の模様を指紋パターン読み取り機６で読み込み、その画像をＦＦＴ７で周波数ドメインの情報に変換すると、指紋パターン＋ＩＤ情報周波数スペクトラム２０のように示される。次に、図４に示すように、自分の指紋パターン１２をＦＦＴ１１で周波数ドメインに変換すると、指紋データ周波数スペクトラム２２に示されるようになり、減算器８で、指紋パターン＋ＩＤ情報の周波数スペクトラム２０から、指紋データ周波数スペクトラム２２を減算すると、図５に示す様に周波数数成分の強いところに、ＩＤ情報２１に示される様に、ＩＤ情報２１の部分だけ抽出される。このＩＤ情報２１だけのスペクトラムを、例えば４ビット×３ケ、３ビット×４ケ、２ビット×４ケに分けて、予めカードに書き込んだ時の順番と逆の手順でデータを並べ替えて、３２ビットのＩＤ情報に戻す。

【００５６】また、図１に示すように、カードの磁気読み取り機１で、磁気データを読み出し、この情報を復号化処理２で符号を解読し、３２ビットのＩＤ情報３を抽出する。

【００５７】次に、カード２５の指紋パターンの模様から抽出した３２ビットのＩＤ情報９とカードの磁気データから抽出した３２ビットのＩＤ情報３とを比較器４で比較し、同一のＩＤ情報であれば”０”を出力し、異なる場合は”１”を出力する。この値を判定回路５において、”０”の時は正規のカードであるため、通常のカード処理に引き続き移行し、”１”の時は不正に複製されたカードであるためカードの処理を中止する作業を行う。

【００５８】［第３の実施形態］次に、本発明の第２の実施の形態について図面を参照して説明する。図６を参照すると、図１と基本的には原理は同じで、図１のＦＦＴに相当する部分にＪＰＥＧ等の画像圧縮で使用しているＤＣＴ（離散コサイン変換）を用いる。このＤＣＴは、直交変換符号化の一種で、ＤＦＴ（Discrete Fourier Transform）の改造版で、８画素×８画素のブロック毎に直交変換行列で変換し変換結果を量子化して符号化データに置き換えて符号化する。このＤＣＴはＦＦＴと同様にバタフライ演算で演算処理を高速化でき、画像成分の高域成分の少ない特性を利用している。本実施形態で用いるＤＣＴには、非線形量子化して等長符号化する方式や準線形量子化して可変長符号化する方式のいずれでもよい。なお、画像圧縮するブロックによって符号化誤差が違うとそのブロックが画面上でブロック歪として現れるので、このブロック歪が目立ちやすい画面の場合には符号化速度を高くし、目立たない画面の場合には符号化速度を低くして全体を通しての画質を一定にできるという特質を有している。

【００５９】このＤＣＴ２３，２４のデータ変換時、第１の実施形態では、指紋パターンの全ての情報に対して周波数ドメインの変換をしていたが、第２の実施形態では、カードの模様を作る時に、予め自分の指紋パターンを８×８ドットの細かい画像（ブロック）に分けてから、ＤＣＴを用いて刷り込んでおく。この場合、ＩＤ情報９は、指紋パターンを８×８ドットに細かく分けた領域全てにＩＤ情報が刷り込まれている為、カードに傷がついたり、自分の指紋に多少の傷が有っても、傷の付いていない部分のデータの相関関係により、たとえば多数決処理には、ある程度の傷で有ればＩＤ情報を抽出することが出来るという新たな特徴が生まれる。

【００６０】また、指紋パターンのＦＦＴ又はＤＣＴによる画像信号の周波数スペクトラムの特定周波数成分にＩＤ情報を加算する例を示したが、指紋パターンの特徴的な領域と範囲を特定することで、現実の指紋採取時の指紋パターンの取得領域や範囲を合わせる必要があるが、この点は、指紋読み取り器１０の採取特性に従うことで解決できる。

【００６１】［第４の実施形態］本発明の第４の実施形態は、磁気カードＩＤ情報暗号化方式に関するもので、カード型記録媒体として、磁気カードを用いる。

【００６２】図７は、磁気カードＩＤ情報暗号化方式の構成を示すブロック図である。本実施形態の磁気カードＩＤ情報暗号化方式は、磁気カードに印刷される模様の元になる原画パターン３１をＦＦＴ（高速フーリエ変換）して、周波数ドメインの情報（原画像周波数スペクトラム３９。図８参照）に変換するＦＦＴ手段３２と、当該磁気カードのユーザを特定するＩＤ情報３６を周波数ドメインに分布させた情報（ＩＤ情報周波数スペクトラム４１。図８参照）を生成して原画像周波数スペクトラム３９とＩＤ情報周波数スペクトラム４１とを加算する加算手段３３と、加算手段３３による加算によって生成された周波数ドメインの情報である原画像＋ＩＤ情報周波数スペクトラム４０（図８参照）を２次元の画像パターンに戻す逆ＦＦＴ手段３４と、逆ＦＦＴ手段３４によって生成された画像パターンを当該磁気カードの模様（図１０参照）として使うように当該磁気カードに印刷する画像パターン印刷手段３５と、ＩＤ情報３６の内容

を暗号化する暗号化手段３７（暗号化の態様は問わない）と、暗号化されたＩＤ情報３６を磁気情報として当該磁気カード上の磁気ストライプ（図１０参照）等の磁気記録部分に書き込む磁気情報作成手段３８とを含んで構成されている。

【００６３】ここで、暗号化手段３７による暗号化の態様として、対称暗号系（慣用暗号系）によるＤＥＳ，ＭＵＬＴＩ２等のブロック暗号やバーナム暗号，入替え暗号等の同期式等のストリーム暗号でもよく、非対称暗号系（公開鍵暗号）によるＲＡＳ，Ｒａｂｉｎ等のベキ乗剰余型暗号やナップザック型暗号等であってもよく、特に使用の制限がなければ、限定されるものではない。

【００６４】以下に、図７中の構成要素について説明を加える。ＦＦＴ手段３２は、例えば２５ポイントの周波数帯域に分けるＦＦＴを行う。ここで、各周波数帯域当たりの量子化数は、例えば１６ビットとする。暗号化手段３７は、例えば３２ビットのＩＤ情報３６を暗号化する（後述の図９参照）。

【００６５】なお、暗号化手段３７と磁気情報作成手段３８とは、上述の第１の従来技術で説明した同名の手段（図２０参照）と同一の手段であってもよい。

【００６６】図８は、本実施例の磁気カードＩＤ情報暗号化方式の原理を説明するための図である。また、図９は、加算手段３３の処理（ＩＤ情報３６の分割処理等）を説明するための図である。

【００６７】さらに、図１０は、本実施形態の磁気カードＩＤ情報暗号化方式によって製造される磁気カード４２の一例を示す図である。磁気カード４２には、ＩＤ情報を刷り込んだ模様４４と、ＩＤ情報を暗号化したデータを記録した磁気ストライプ４３から構成されている。この磁気カード４２の所有者は、自分自身を証明する身分証明書や銀行用のキャッシュカード、クレジットカード等に個別に、又は統括的に所持して提示することによって種々使用できる。

【００６８】また、図１１は、本実施形態の磁気カードＩＤ情報暗号化方式の処理を示す流れ図である。この処理は、ＦＦＴステップ５０１と、ＩＤ情報周波数スペクトラム生成ステップ５０２と、原画像＋ＩＤ情報周波数スペクトラム生成ステップ５０３と、逆ＦＦＴステップ５０４と、画像パターン印刷ステップ５０５と、暗号化ステップ５０６と、磁気情報記録ステップ５０７とからなる。

【００６９】次に、このように構成された本実施例の磁気カードＩＤ情報暗号化方式の動作について、図７～図１１を参照して詳細に説明する。

【００７０】まず、磁気カードに印刷される模様の元となる原画パターン３１が用意される。このときに、この原画パターン３１は、後で周波数ドメインの情報に変換した時に、ＩＤ情報３６を加算してもオーバフローしないものを予め準備しておく。

【００７１】ＦＦＴ手段３２は、この原画パターン３１に対して、周波数ドメインの情報になるように、高速フーリエ変換（ＦＦＴ）を行う（図１１のステップ５０１）。これによって、図８に示すように、原画パターン３１は原画像周波数スペクトラム３９に変換される。

【００７２】加算手段３３は、ＦＦＴ手段３２によって生成された原画像周波数スペクトラム３９の分布状況を見て、図８や図９に示すように、ＩＤ情報周波数スペクトラム４１を生成する（ステップ５０２）。すなわち、本実施形態のようにＩＤ情報３６が３２ビットである場合には、この３２ビットを４ビット×３，３ビット×４，および２ビット×４というように分けて、原画像周波数スペクトラム３９の分布状況に類似させて、ＩＤ情報周波数スペクトラム４１を生成する。即ち、原画パターン３１の周波数成分のエネルギーがより強い部分から順番に、分割したＩＤ情報３６のビット数のより多い部分を分布させて、ＩＤ情報周波数スペクトラム４１を生成する。ただし、このような「原画像周波数スペクトラム３９の分布状況とＩＤ情報周波数スペクトラム４１の分布状況とを類似させる処理」を行わなくても、本実施形態を実現することは可能である。

【００７３】次に、加算手段３３は、図８に示すように、原画像周波数スペクトラム３９とＩＤ情報周波数スペクトラム４１とを加算して、原画像＋ＩＤ情報周波数スペクトラム４０を生成する（ステップ５０３）。

【００７４】この場合に、原画像周波数スペクトラム３９のエネルギーに比べてＩＤ情報周波数スペクトラム４１のエネルギーは微小なものとなるように設定されているので、磁気カード上の模様となる画像パターンに対してＩＤ情報３６（ＩＤ情報周波数スペクトラム４１）の存在はほとんど影響を与えない。また、本実施形態では、原画像周波数スペクトラム３９とＩＤ情報周波数スペクトラム４１との両方の分布状況ができるだけ類似した形状とされるので（図８参照）、磁気カードの模様の画像パターンに及ぼされるＩＤ情報３６の影響は、さらに小さくなる。

【００７５】逆ＦＦＴ手段３４は、ステップ５０３で生成された原画像＋ＩＤ情報周波数スペクトラム４０に対して逆ＦＦＴを行い、原画像＋ＩＤ情報周波数スペクトラム４０を画像パターンに戻す（ステップ５０４）。ここでできた画像パターンは、上述のように、見た目では原画パターン３１と非常に区別がつきにくい画像パターンになる。

【００７６】画像パターン印刷手段３５は、この画像パターンを模様として磁気カードに印刷する（ステップ５０５）。このように作成（印刷）された磁気カードの模様は、原画パターン３１が同一であればＩＤ情報３６が異なっても全て同じように見える。

【００７７】一方、暗号化手段３７は、磁気カードに記録する磁気情報を従来技術によって作成する要領で（図

２０参照）、ＩＤ情報３６のデータを分析しにくくする暗号化を行う（ステップ５０６）。

【００７８】磁気情報作成手段３８は、ステップ５０６で暗号化されたＩＤ情報を示す磁気情報を磁気カード上の磁気記録部分（図１０中の磁気ストライプ）に書き込む（ステツプ５０７）。以上で、磁気カードのＩＤ情報３６が、磁気情報と模様との両方の態様で記録／印刷される（刷り込まれる）。

【００７９】上記実施形態では、記録媒体の磁気カードに原画パターンにＩＤ情報を加算して、表面的に見える磁気カードの画像信号には原画パターンと殆ど見分けのつかないようにしているが、この暗号化された磁気カードは、特定の解読器によってＩＤ情報を読み取り、現実の磁気カードの所持者が示すＩＤ情報と一致するのかどうかで正規か、又は不正に磁気カード保持者かが判断できる。

【００８０】［第５の実施形態］本発明の第５の実施形態による磁気カードＩＤ情報暗号化方式について、説明する。

【００８１】図１２は、本発明の磁気カードＩＤ情報暗号化方式の第５の実施形態の構成を示すブロック図である。本実施形態の磁気カードＩＤ情報暗号化方式は、磁気カードに印刷される模様の元になる原画パターン６１をＤＣＴで周波数ドメインの情報に変換するＤＣＴ手段６２と、当該磁気カードのユーザを特定するＩＤ情報６６を周波数ドメインに分布させた情報を生成して、当該生成情報とＤＣＴ手段６２によって生成された周波数ドメインの情報とを加算する加算手段６３と、加算手段６３による加算によって生成された周波数ドメインの情報を逆ＤＣＴによって２次元の画像パターンに戻す逆ＤＣＴ手段６４と、逆ＤＣＴ手段６４によって生成された画像パターンを当該磁気カードの模様として使うように当該磁気カードに印刷する画像パターン印刷手段６５と、ＩＤ情報６６の内容を暗号化する暗号化手段６７（暗号化の態様は問わない）と、暗号化されたＩＤ情報６６を磁気情報として当該磁気カード上の磁気ストライプ等の磁気記録部分に書き込む磁気情報作成手段６８とを含んで構成されている。

【００８２】なお、本実施形態における加算手段６３，画像パターン印刷手段６５，暗号化手段６７，および磁気情報作成手段６８は、第４の実施形態における加算手段３３，画像パターン印刷手段３５，暗号化手段３７，および磁気情報作成手段３８と同様の手段である。

【００８３】図１２に示すように、本実施形態の磁気カードＩＤ情報暗号化方式の原埋は、図８に示す第４の実施形態の原理と基本的には同じである。ただし、本実施例では、図７中のＦＦＴ手段３２に相当する部分にＪＰＥＧ（Joint Photographic Coding Experts Group）等の画像圧縮で使用されているＤＣＴ（後述のように、原画パターン６１を細分化原画パターンに細分化した上でのＤＣＴ）を行うＤＣＴ手段６２が用いられ、逆ＦＦＴ手段３４に相当する部分に逆ＤＣＴを行う逆ＤＣＴ手段６４が用いられる。

【００８４】次に、本実施形態に特徴的な動作について、詳細に説明する。第４の実施形態におけるＦＦＴ手段３２は、原画パターン３１の全ての情報を対象として周波数ドメインの情報への変換を行っていた。しかし、本第２の実施形態におけるＤＣＴ手段６２は、原画パターン６１を８×８ドットの細かい画像パターンである細分化原画パターンに分けて、各細分化原画パターンに対してＤＣＴを行う。

【００８５】また、加算手段６３は、ＩＤ情報６６を周波数ドメインに分布させた上で、その周波数ドメインのＩＤ情報６６を各細分化原画パターンにＤＣＴが施された情報のそれぞれに加算する。

【００８６】本実施形態の磁気カードＩＤ情報暗号化方式では、上述のように細分化原画パターンの全てにＩＤ情報６６が刷り込まれるため、磁気カードに部分的に傷がついて一部の画像のデータがおかしくなっても、傷のついていない画像の部分には依然として正確なＩＤ情報６６が刷り込まれたままとなるという特長が生まれる。

【００８７】上記磁気カードＩＤ情報暗号化方式の解読方式の一例を、図１３に示して説明する。正確なＩＤ情報６６が刷り込まれた模様４４の画像データとＩＤ情報を暗号化したコードとして記録されている磁気ストライプ４３を含むカード型記録媒体４２を磁気カード情報解読器の所定の個所に挿入する。磁気読取部８１では、磁気カード４２と相対的に移動する磁気ヘッドで磁気ストライプ４３に記録されている記録コードを電気信号に変換する。記録コードは逆暗号化手段８２で上記暗号化手段６７で暗号化した方式と逆の方式で暗号化を正規のＩＤ情報信号に変換し、ＩＤ情報８３を得る。一方、画像読取部８４では、予め定められた模様４４の領域を光電変換素子で直接又は、縮尺して画像信号として読み取る。当該画像信号は小ブロック毎に、上記ＤＣＴ手段６２と同様に、ＤＣＴ手段８５でＤＣＴを行い、次に、ＤＣＴされた画像信号は、ＩＤ情報８３の周波数スペクトラム化したデータから差を取られ、逆ＤＣＴ手段８７で先のＤＣＴ手段８５と逆の変換を行い、抽出パターン８８を得ることができる。

【００８８】次に、例えばこのカード型記録媒体を所持する人の顔を写真撮影等で取得したり、著作物の原画そのものを原画パターン８９としてデジタル変換し、抽出パターンのデジタル信号と比較器９０で比較する。この比較の結果、両者に差異がなく同一模様であると判断された場合には、正規のカード保持者であると認証される。また、両者の差異が大きかった場合には、正規のカード保持者ではないと判断される。

【００８９】この際、検出されたＩＤ情報８３と、本磁気カードの所有者が示すＩＤ情報とが一致しておれば、

当該原画パターンの所有者が一致していると判断できる。他方、一致しなければ、本磁気カードの所有者は拾得された磁気カードか、不正行為の所有者と判断できる。このように、例えば原画パターンそのものが貴重な著作権を有する著作物であれば、その原画パターンが上述したように本磁気カードに刷り込まれている場合には、真の所持者であるのかどうかを即座に判断でき、磁気カードの偽造及び不正使用を摘出し、セキュリティの向上に寄与できる。

【００９０】上記暗号解読器は、図１２に示す磁気カードＩＤ情報暗号化方式に対応する例を示したが、図７に示す第４の実施形態の磁気カードＩＤ情報暗号化方式であっても、ＤＣＴ手段８５と逆ＤＣＴ手段８７とを、ＦＦＴ手段３２と逆ＦＦＴ手段３４に変更することで、解読することができる。

【００９１】［第６の実施形態］図１４は、本発明の第６の実施形態のカード型記録媒体の一種の身分証明書を作成する構成と信号経路を示し、図１５は、本発明の第６の実施形態の身分証明書を検査する検査工程とその構成図である。図１６は、本発明の第６の実施形態の身分証明書を発行するためのシステムを示し、図１７は、本発明の第６の実施形態の身分証明書を検査するシステムを示す。

【００９２】図１４において、写真１００は、身分証明書の正規の所有者の写真である。記載事項１１０は当該身分証明書２２０に記載される事項で、公務員や会社社員用身分証明書の場合には、所有者の名前、部署の名前、登録番号や社員番号などが記載される。学生用身分証明書の場合には、所有者の名前、学部の名前、学生番号などが記載される。キャプチャ１２０は、写真１００を画像データとして取り込む画像読み取る部分である。識別データ生成部１３０は、身分証明書２２０の記載事項１１０から計算によって識別データを生成する。生成の方法としては、名前や社員番号に基づいて乱数を発生させる方法が使用できる。ＤＣＴ部１４０は、キャプチャ１２０で取り込まれた画像データを空間周波数成分に変換する機能を有する。部分平均計算部１５０は空間周波数成分の近傍３点の絶対値の平均を計算する。この部分平均は乗算器１６０で識別データと乗算され、この乗算結果は乗算器１８０で定数αでα倍される。乗算器１８０出力は、加算器１９０で、ＤＣＴ部１４０の出力と加算され、この加算結果はＩＤＣＴ（Inverce Discrete Cosine Transform）部２００に供給される。定数αはスケーリングファクタである。ＩＤＣＴ部２００は空間周波数から人間の目に見える画像データに変換する機能を有する。写真２１０は識別データが埋め込まれている写真であり、この写真２１０と記載事項１１０を印刷したものが身分証明書２２０である。

【００９３】次に、作成された身分証明書を現実の使用状態に置かれたときの証明・検査手段について説明する。図１５において、身分証明書３００は、識別データが埋め込まれている写真と、識別データを生成するもとになった記載事項とともに印刷された身分証明書である。キャプチャ３１０は、この身分証明書の写真の画像部分を光電変換して読み込んで、写真の部分は画像データとして、記載事項の部分も画像データとして分離する機能を有する。ＤＣＴ部３２０は、キャプチャ３１０で分離された画像データを空間周波数成分に変換する機能を有する。文字認識部３３０は、キャプチャ３１０から分離された記載事項部分の画像データから文字認識を用いて、記載事項を文字に変換する。部分平均計算部３４０はこの空間周波数成分で近傍３点の絶対値の平均値を計算する。

【００９４】また、識別データ生成部３７０は、キャプチャ３１０から分離された記載事項のデータを元に識別データを計算する。内積計算部３８０は画像の空間周波数成分から抜き出した識別データと記載事項から生成した識別データとの内積を計算する機能を有する。なお、除算器３５０、加算器３６０の動作は後述する。

【００９５】以下、身分証明書の作成動作、検査動作をより具体的に詳細に説明する。まず、身分証明書作成の方から説明する。身分証明書を作成する必要のある者が写真１００と、識別データを作成する為に必要な記載事項を用意する。ここでは記載事項を社員番号とする。身分証明書作成担当者は、図１６（ａ）のカメラ８００、または、スキャナ８１０で写真１００を画像処理装置８３０に取り込む。

【００９６】また、記載事項１１０はキーボード８２０から身分証明書作成担当者が入力する。画像処理装置８３０に取り込まれた写真１１０の画像データ、及び、記載事項データ１１０は、図１４の流れにそって処理される。取り込まれた画像データはＤＣＴ部１４０で空間周波数成分に変換される。識別データ生成部１３０ではキーボード８２０から入力された記載事項データに基づいて平均０、分散１の正規分布の識別データを生成する。空間周波数成分に変換されたデータと識別データとの間で次の計算を行って、識別データを埋め込む。

【００９７】ＤＣＴ部１４０のＤＣＴ後の空間周波数成分の低いものから順に、

ｆ（１），ｆ（２），…，ｆ（ｎ）、

識別データを

ｗ（１），ｗ（２），…，ｗ（ｎ）

とし、

Ｆ（ｉ）＝ｆ（ｉ）＋α×ａｖｇ（ｆ（ｉ））×ｗ（ｉ）

を各ｉについて計算する。部分平均ａｖｇ（ｆ（ｉ））は前述の部分平均計算部１５０で計算される。

【００９８】ＩＤＣＴ部２００は計算結果のＦ（ｉ）を逆コサイン変換して、識別データが埋め込まれた状態の写真２１０を作成する。写真２１０と記載事項１１０は

印刷装置８４０で身分証明書に印刷され、身分証明書２２０ができあがる。

【００９９】なお、図１６（ａ）において、ＲＯＭ８３５には、図１６で示した画像処理装置８３０の処理を実行させるためのプログラムが格納されている。このＲＯＭ８３５はハードディスクやフロッピーディスク等でも代替できる。

【０１００】次に、身分証明書を検査する方を説明する。識別データが埋め込まれた写真と記載事項との両方が印刷された身分証明書を、図１６（ｂ）のカメラ８５０で読み込んで、検査装置８７０に入力する。検査装置８７０に取り込まれたデータは、図１５の流れにそって処理される。読み込まれた画像データは、キャプチャ３１０で写真の部分と記載事項の部分に分離され、それぞれＤＣＴ部３２０、文字認識部３３０に出力される。ＤＣＴ部３２０は入力されたデータを空間周波数に変換する。

【０１０１】ＤＣＴ部３２０で空間周波数変換後の周波数成分の低いものから順に

Ｆ（１），Ｆ（２），…，Ｆ（ｎ）

とする。部分平均計算部３４０は、Ｆ（ｉ）の近傍３点の絶対値の部分平均ａｖｇ（Ｆ（ｉ））を計算する。画像データから抜き出す識別データをＷ（ｉ）とし、

Ｗ（ｉ）＝Ｆ（ｉ）／ａｖｇ（Ｆ（ｉ））により計算する。加算器３６０はこのＷ（ｉ）について、画像全体の総和ＷＦ（ｉ）をｉ毎に計算する。

【０１０２】一方、文字認識部３３０は、記載事項部分の画像データから文字認識にて記載事項を文字として再生する。識別データ生成部３７０は文字認識部３３０からの記載事項データに基づいて、平均０、分散１の正規分布の識別データを生成する。

【０１０３】つぎに、内積計算部３８０は、識別データＷ（ｉ）とＷＦ（ｉ）のベクトル内積を計算する。すなわち、

Ｃ＝（ＷＦ×ｗ）／（ＷＦＤ×ｗＤ）

を計算する。ここで、

ＷＦ＝（ＷＦ（１），ＷＦ（２），…，ＷＦ（ｎ））、

ｗ＝（ｗ（１），ｗ（２），…，ｗ（ｎ））、

ＷＦＤはベクトルＷＦの絶対値、ｗＤはベクトルｗの絶対値である。このＣがある値以上である場合は、写真に埋め込まれた識別データと記載事項との間に相関関係があると判断され、この身分証明書は真正のものであるとディスプレイ８８０に表示される。

【０１０４】なお、図１６（ｂ）において、ＲＯＭ８７５には、図１５で示した動作を検査装置８７０に実行させるためのプログラムを格納している。

【０１０５】次に、偽造された場合はどうなるか説明する。一番簡単な偽造方法は写真のみを貼りかえることである。ところが、検査の段階で画像データから抜き取った識別データと記載事項から生成した識別データとで相関関係を求めたときに、前述のＣの値がほとんどゼロになる。なぜなら、写真の中には記載事項に基づいて生成された識別データが埋め込まれていないからである。したがって、容易に偽造身分証明書として判断することが可能である。

【０１０６】次に考えられる偽造方法は、記載事項から識別データを生成して写真に埋め込み、これを印刷して偽造する場合である。この場合は、識別データを生成する乱数の計算式がわからないので、正規の場合と違う識別データを生成することになり、検査段階での相関関係を示すＣの値がゼロになり、偽造身分証明書と判断することが可能である。

【０１０７】さらに考えられる偽造方法は、写真の１画素１画素を丹念に調べて識別データを取り出し、計算式を割り出す方法である。この場合は、識別データが挿入されるのは空間周波数成分に分解された時であり、これをＩＤＣＴした後の写真では調べることは不可能である。つまり、特定の画素の部分に識別データが埋め込まれているわけではないからである。

【０１０８】上記実施形態では、電子透かし方式に、更に解読の困難な方式を用いたが、更にデータ・ハイディング方式として、損失を伴うデータ圧縮手法（Lossy Compression）や情報損失を伴わないデータ圧縮手法（Lossless Compression）やスペクトラム拡散技術を用いてさらに解読の困難な方式、即ち、それだけ偽造の困難な方式としてもよい。

【０１０９】［第７の実施形態］次に本発明の第７の実施形態について説明する。図１７は、本発明の第７の実施形態におけるカード型記録媒体の一種の身分証明書を作成する流れを示し、図１８は、本発明の第７の実施形態における身分証明書を検査する流れである。図１９の（ａ）は、本発明の第７の実施形態の身分証明書を発行するためのシステムを示し、図１９の（ｂ）は、本発明の第７の実施形態の身分証明書を検査するシステムを示す。

【０１１０】第７の実施形態では、身分証明書５２０に磁気記録部分５３０を設け、この磁気記録部分に名前や社員番号を記録し、身分証明書の表面にはこれらを記載しないようにしたものである。つまり、図１７、図１９（ａ）に示すように、識別データを埋め込んだ写真を作成するところまでは、第６の実施形態と同じであるが、身分証明書にする際には、写真１００は表面に印刷し、名前や社員番号の記載事項１１０は、一方は識別データとして写真の画像データに埋め込むが、他方は識別データを直接に、又は暗号化して磁気記録データに変換し、磁気記録部分５３０に磁気カードライター９５０を使用して記録する。

【０１１１】つぎに、検査装置の方は、図１８，図１９（ｂ）に示すように、身分証明書６００内の写真は第６の実施形態と同じで、カメラ８５０で読み込み、名前な

どの情報は磁気記録部分６１０から磁気カードリーダー９７０を経由して読み込む。読み込んだあとの処理は第６の実施形態と同じで、写真をキャプチャ３１０で画像データに変換し、これを各ブロック毎にＤＣＴ変換して、ＤＣＴデータをこれの部分平均で除算し、この結果を加算して画像全体の総和ＷＦ（ｉ）を求め、磁気カードに記録された識別データのベクトル内積を計算する。この結果で正規の所持者か、又は不正に改造した身分証明書かを判断する。この様に、磁気カードの磁気ストライプ部に識別データ、又は識別データを暗号化したデータを記録するので、こうすることにより、識別データを作成する元となる名前などのデータがわかり難くなり、より偽造することが困難になる。

【０１１２】上記実施形態では、電子すかし技術を利用して、更に偽造を困難とするもので、上記身分証明書には、顔写真に識別コードを透かしこんだ例を示したが、顔写真に限らず個人を特定できる指紋や目の網膜網を用いてもよく、識別コードの代わりに個人の記憶を尊重するＩＤ情報としてもよい。

【０１１３】また、上記各実施形態では、カード型記録媒体に、画像情報と識別ＩＤ情報とを暗号化技術とを組み合わせて、本人の所持するカードと真のカード所持者の一致を第１目的としているが、クレジットカードやテレホンカード、キャッシュカード、社員カード、学生カード、健康保険カードなど今後発行される新規のカードをも含めて、多数のカードに適用できるものである。また、基本的に磁気ストライプに書き込んで読み出す磁気を利用したものがローコストで信頼性も高いが、記録方式には、光学的方式、光磁気方式等、他の方式であっても本発明を利用することができ、上記実施形態に限られるものではないことは明らかである。

【０１１４】

【発明の効果】本発明によれば、磁気カードの情報とＩＤ情報を刷り込んだ画像情報の二重でＩＤ情報を照合出来るということである。これにより、カードを判断する時に、不正にカードを複製したのか、オリジナルのカードであるのか判断し易くなる。その理由は、磁気カードの磁気の部分の他にＩＤ情報が入っているとは悟られないように、カードの模様にＩＤ情報を刷り込むようにしたからである。

【０１１５】また、磁気カードの磁気の部分のデータが壊れてもＩＤ情報の確認が容易に確認することが可能ということである。これにより、外部からの磁気の影響で磁気データが壊れても、模様の部分にＩＤ情報が刷り込んである為、その情報を読み取って、オリジナルのカードであるか判別することが出来るようになる。その理由は、模様の部分は磁気の影響を受けずＩＤ情報が壊れないようになっているからである。

【０１１６】さらに、本発明によると、磁気情報と画像情報との二重の形態て磁気カードにＩＤ情報を記録／印刷することができるので、当該磁気カードの複製が困難になり、第三者による磁気カードの偽造を防ぐことができるということである。このような効果が生じる理由は、磁気カードの磁気記録部分の他にＩＤ情報が入っているとは悟られないように磁気カードの模様にＩＤ情報を刷り込むようにできるからである。すなわち、本発明の磁気カードＩＤ情報暗号化方式によって製造された磁気カードは、磁気情報だけを複製しても模様の部分を複製しない限り、同一の磁気カードとしてみなされないので、磁気カードの偽造は極めて困難なものとなる。なお、模様にＩＤ情報が入っていることを素人が見分けることは、模様の原画像パターンに係る周波数成分のエネルギーがＩＤ情報に係る周波数成分のエネルギーよりも強いことに起因して非常に難しいものとなる。また、もし仮に、模様の違いが分かったとしても、原画パターンがない限り、誰も摸倣することは不可能である。

【０１１７】また、磁気カードの磁気記録部分のデータが壊れてもＩＤ情報の確認を容易に行うことが可能になるということである。これにより、外部からの磁気の影響で磁気情報が壊れても、模様の部分に刷り込んであるＩＤ情報を読み取って磁気情報のＩＤ情報を元に戻すことが簡単にできるようになる。このような効果が生じる理由は、模様の部分は磁気の影響を受けず磁気的原因では模様に刷り込まれたＩＤ情報が壊れないようになっているからである。

【０１１８】さらにまた、この発明を用いるとカード型記録媒体の一種の身分証明書を偽造することは困難である。たとえ、身分証明書の顔写真を張り替えたとしても、又は顔写真の画像に識別コードを埋め込んだりして偽造されたとしても、簡単に識別することができる。

【０１１９】また、本発明による記録媒体には、カード型記録媒体の検査システムをマイクロコンピュータ等にて同一手順で動作させ得るプログラムを格納しているので、指紋や顔等の個人情報の特定ばかりでなく、著作物等の管理にも簡単な設備で適用できる。

【図面の簡単な説明】

【図１】本発明のカード型記録媒体の判定手段のブロック図である。

【図２】本発明の実施形態のカード作成フローである。

【図３】本発明の実施形態のカード図である。

【図４】本発明の原理図である。

【図５】本発明の実施形態のＩＤ情報抽出図である。

【図６】本発明の一実施形態のブロック図である。

【図７】本発明の磁気カードＩＤ情報暗号化方式の第１の実施形態の構成を示すブロック図である。

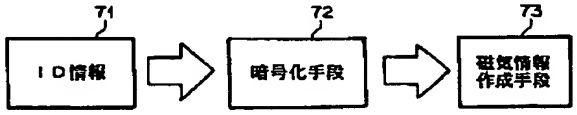
【図８】図７に示す磁気カードＩＤ情報暗号化方式の原理を説明するための図である。

【図９】図７中の加算手段による処理（ＩＤ情報の分割処理等）を説明するための図である。

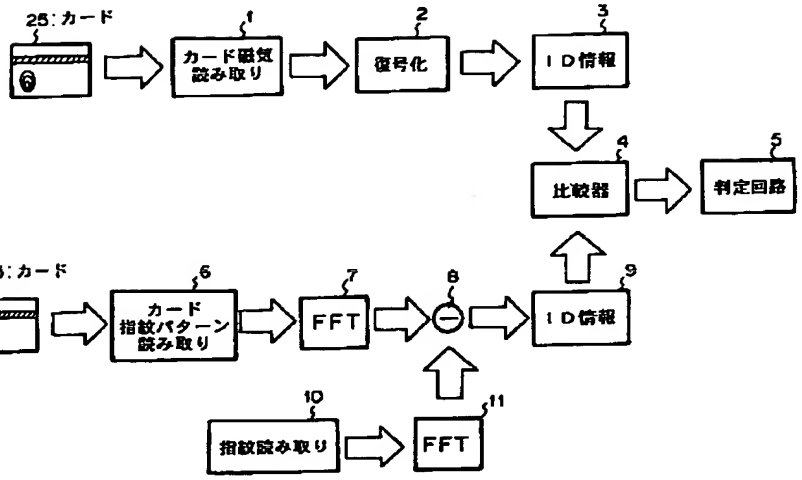
【図１０】図７に示す磁気カードＩＤ情報暗号化方式に

よって製造される磁気カードの一例を示す図である。
【図１１】図７に示す磁気カードＩＤ情報暗号化方式の処理を示す流れ図である。
【図１２】本発明の磁気カードＩＤ情報暗号化方式の第５の実施形態の構成を示すブロック図である。
【図１３】本発明の磁気カードＩＤ情報暗号化解読器の第５の実施形態の構成を示すブロック図である。
【図１４】本発明の第６の実施形態の身分証明書作成の処理の流れを示す図である。
【図１５】本発明の第６の実施形態の身分証明書検査の処理の流れを示す図である。
【図１６】各々、本発明の第６の実施形態の身分証明書作成システム、身分証明書検査システムの構成例を示す図である。
【図１７】本発明の第７の実施形態の身分証明書作成の処理の流れを示す図である。
【図１８】本発明の第７の実施形態の身分証明書検査の処理の流れを示す図である。
【図１９】本発明の第７の実施形態の身分証明書作成システム、身分証明書検査システムの構成例を示す図である。
【図２０】従来の磁気カードＩＤ情報暗号化方式の一例の構成を示すブロック図である。
【符号の説明】
１　カード磁気読み取り
２　復号化
３　ＩＤ情報
４　比較器
５　判定回路
６　カード画像パターン読み取り機
７　ＦＦＴ（高速フーリエ変換）
８　減算器
９　ＩＤ情報
１０　指紋読み取り
１１　ＦＦＴ
１２　本人の指紋パターン
１３　加算器
１４　逆ＦＦＴ
１５　指紋パターン印刷機
１６　暗号化
１７　磁気テープ作成機
１８　カードの磁気情報
１９　カードの指紋パターン
２０　指紋データ＋ＩＤ情報の周波数スペクトラム
２１　ＩＤ情報の周波数スペクトラム
２２　指紋データの周波数スペクトラム
２３　ＤＣＴ（離散コサイン変換）
２４　ＤＣＴ
３１，６１　原画パターン
３２　ＦＦＴ手段
３３，６３　加算手段
３４　逆ＦＦＴ手段
３５，６５　画像パターン印刷手段
３６，６６　ＩＤ情報
３７，６７　暗号化手段
３８，６８　磁気情報作成手段
３９　原画像周波数スペクトラム
４０　原画像＋ＩＤ情報周波数スペクトラム
４１　ＩＤ情報周波数スペクトラム
６２　ＤＣＴ手段
６４　逆ＤＣＴ手段
１２０，３１０　キャプチャ
１３０，３７０　識別データ生成部
１４０，３２０　離散コサイン変換部（ＤＣＴ）
１５０，３４０　部分平均計算部
１６０，１８０　乗算器
１９０，３６０　加算器
２００　逆離散コサイン変換部（ＩＤＣＴ）
３３０　文字認識部
３８０　内積計算部
３９０　相関比率計算部
６３０　磁気カードリーダー
８００，８５０　カメラ
８１０　スキャナ
８２０，８６０　キーボード
８３０，９３０　画像処理装置
８４０　印刷装置
８３５，８７５，９３５，９９５　ＲＯＭ
８７０，９９０　身分証明書検査装置
８８０　ディスプレイ
９５０　磁気カードライター
９７０　磁気カードリーダー

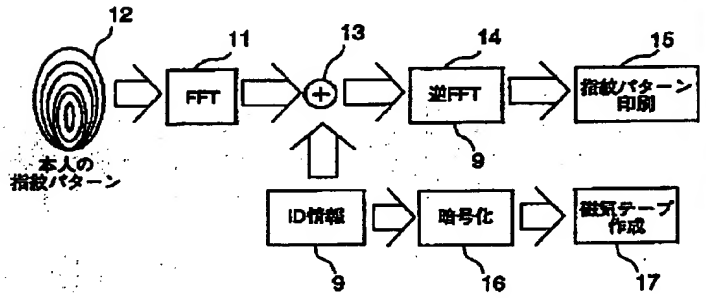
【図２０】



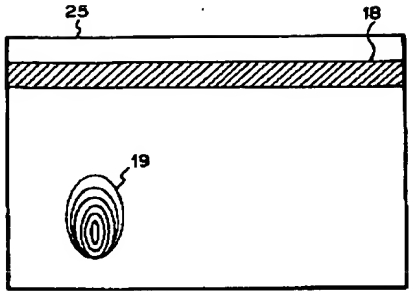
【図１】



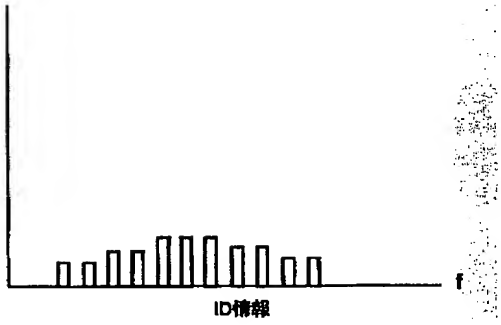
【図２】



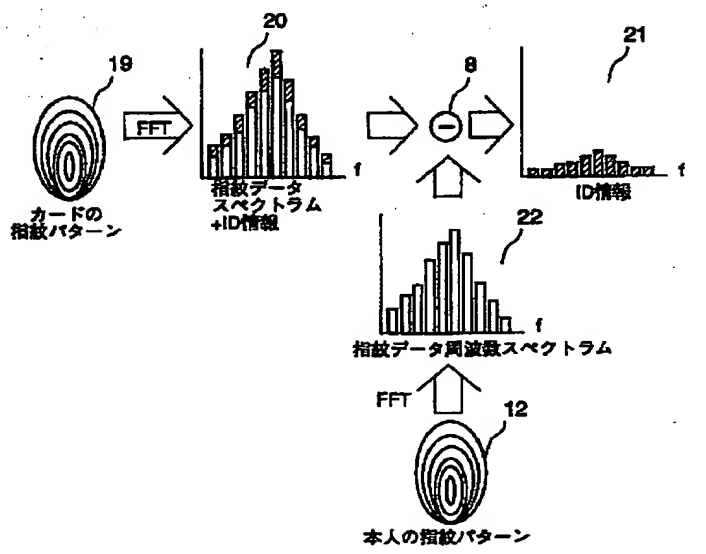
【図３】



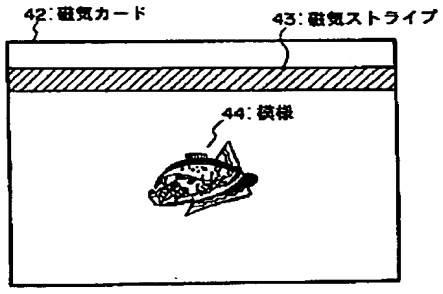
【図５】



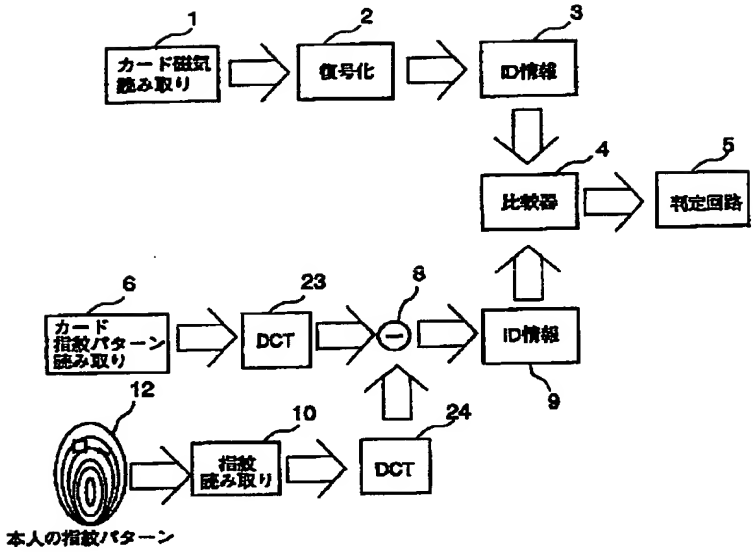
【図４】



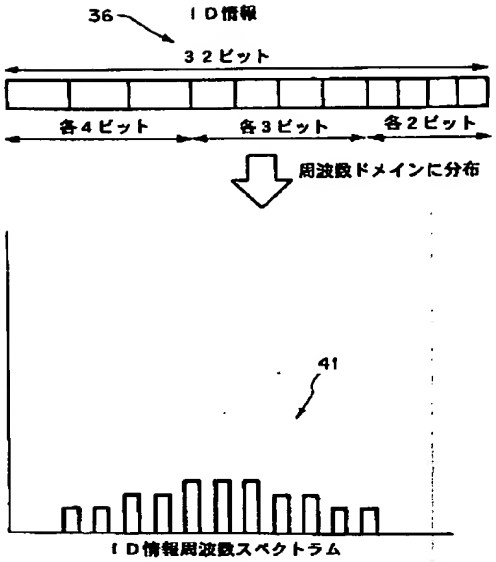
【図１０】



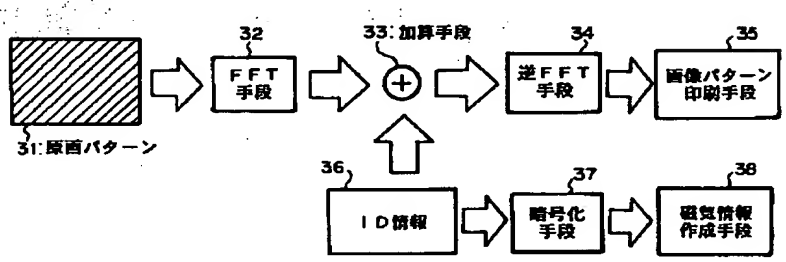
【図６】


1
カード磁気読み取り
2
復号化
3
ID情報
4
比較器
5
判定回路
6
カード指紋パターン読み取り
23
DCT
8
ID情報
9
12
10
指紋読み取り
24
DCT
本人の指紋パターン

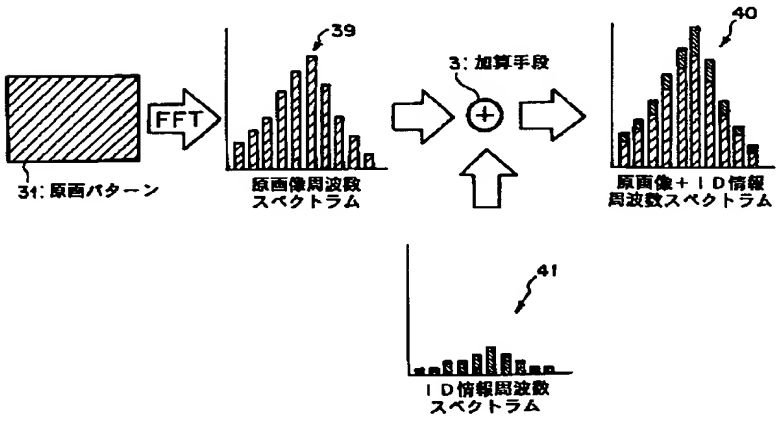
【図９】


36
ＩＤ情報
３２ビット
各４ビット
各３ビット
各２ビット
周波数ドメインに分布
41
ＩＤ情報周波数スペクトラム

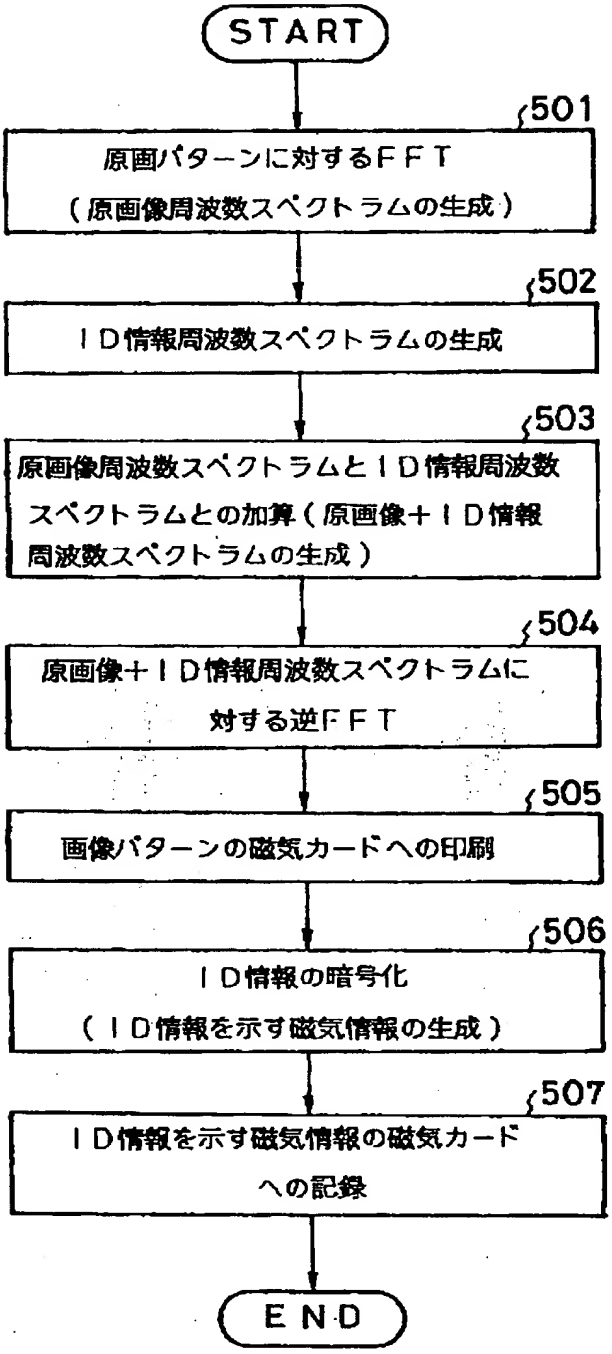
【図７】


32
ＦＦＴ手段
33:加算手段
34
逆ＦＦＴ手段
35
画像パターン印刷手段
31:原画パターン
36
ＩＤ情報
37
暗号化手段
38
磁気情報作成手段

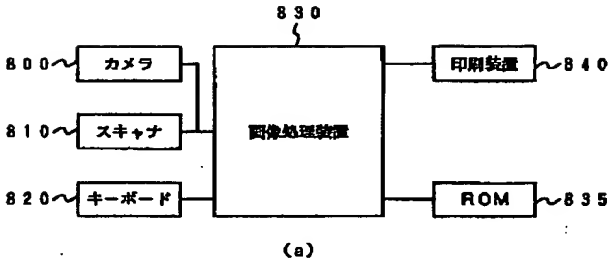
【図８】

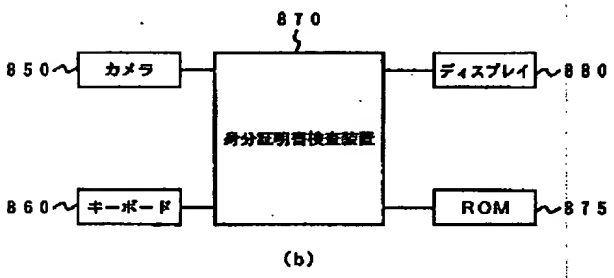

FFT
31:原画パターン
39
原画像周波数スペクトラム
3:加算手段
40
原画像＋ＩＤ情報周波数スペクトラム
41
ＩＤ情報周波数スペクトラム

【図１１】

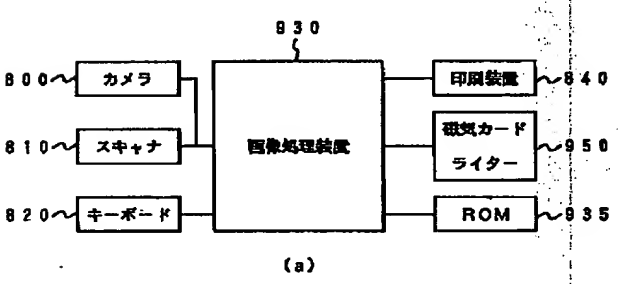

START
501
原画パターンに対するＦＦＴ
（原画像周波数スペクトラムの生成）
502
ＩＤ情報周波数スペクトラムの生成
503
原画像周波数スペクトラムとＩＤ情報周波数スペクトラムとの加算（原画像＋ＩＤ情報周波数スペクトラムの生成）
504
原画像＋ＩＤ情報周波数スペクトラムに対する逆ＦＦＴ
505
画像パターンの磁気カードへの印刷
506
ＩＤ情報の暗号化
（ＩＤ情報を示す磁気情報の生成）
507
ＩＤ情報を示す磁気情報の磁気カードへの記録
END

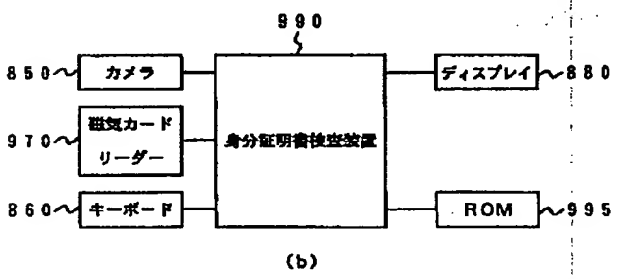
【図１６】


830
800
カメラ
810
スキャナ
820
キーボード
画像処理装置
印刷装置
840
ROM
835
(a)

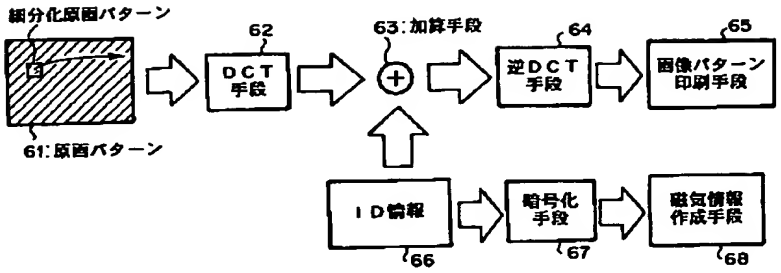

870
850
カメラ
860
キーボード
身分証明書検査装置
ディスプレイ
880
ROM
875
(b)

【図１９】

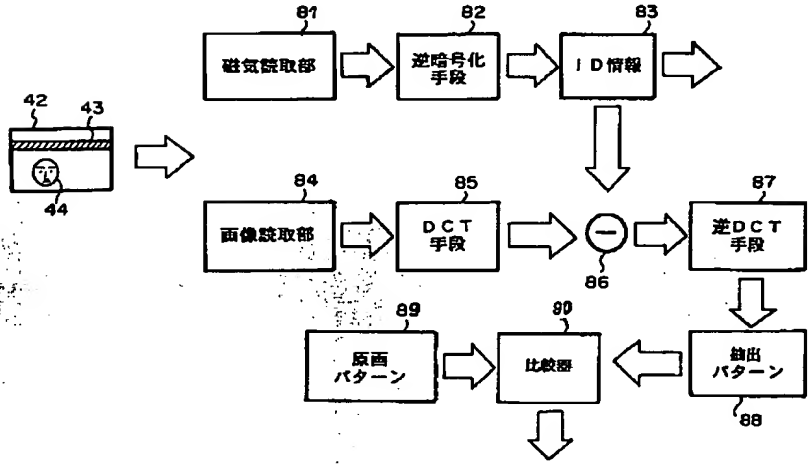

930
800
カメラ
810
スキャナ
820
キーボード
画像処理装置
印刷装置
840
磁気カードライター
950
ROM
935
(a)


990
850
カメラ
970
磁気カードリーダー
860
キーボード
身分証明書検査装置
ディスプレイ
880
ROM
995
(b)

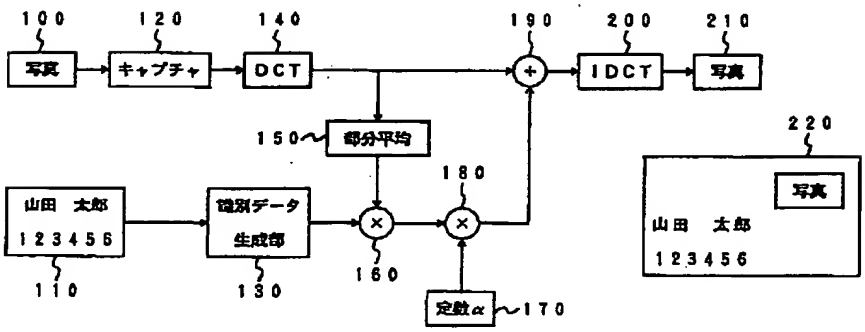
【図１２】


細分化原画パターン
61:原画パターン
62
DCT手段
63:加算手段
64
逆DCT手段
65
画像パターン印刷手段
ID情報
66
暗号化手段
67
磁気情報作成手段
68

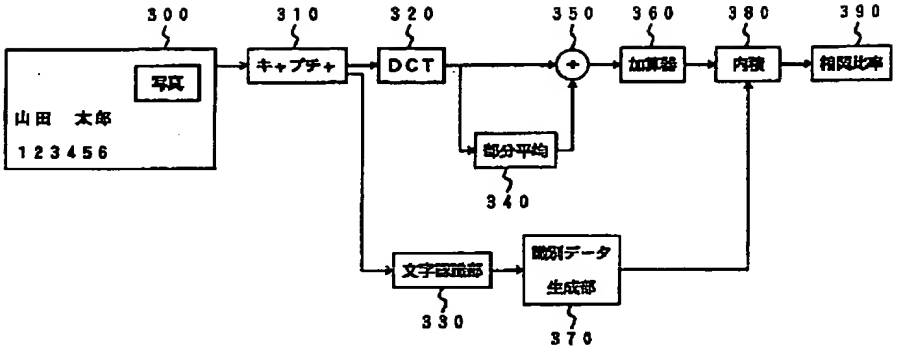
【図１３】


81
磁気読取部
82
逆暗号化手段
83
ID情報
42
43
44
84
画像読取部
85
DCT手段
86
87
逆DCT手段
89
原画パターン
90
比較器
88
抽出パターン

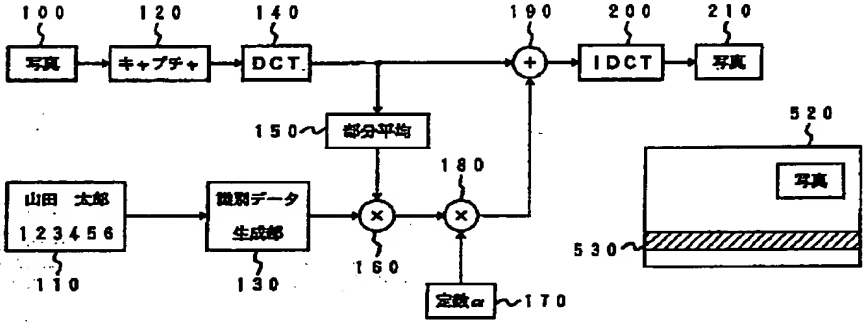
【図１４】


100
写真
120
キャプチャ
140
DCT
190
200
IDCT
210
写真
150
部分平均
180
山田 太郎
123456
110
識別データ生成部
130
160
定数α
170
220
写真
山田 太郎
123456

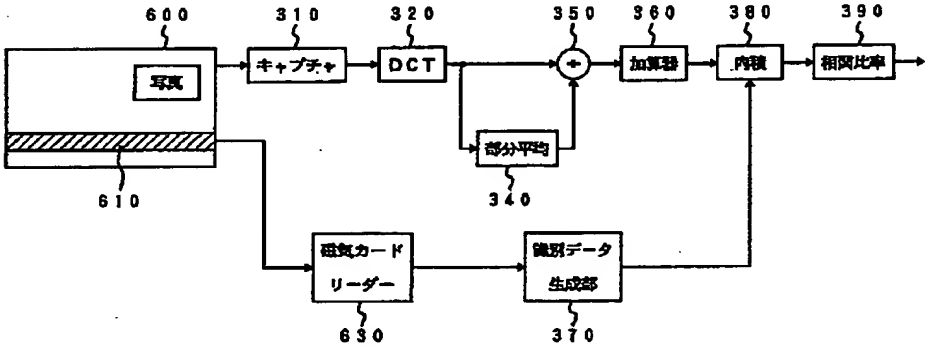
【図１５】



【図１７】



【図１８】



フロントページの続き

(51) Int. Cl.[6]	識別記号	F I	
H04L 9/32		H04L 9/00	673C
			673A
			673E